558,629

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年10 月27 日 (27.10.2005)

PCT

(10) 国際公開番号
WO 2005/101217 A1

(51) 国際特許分類[7]: G06F 13/00, 15/00, H04L 12/46, 12/66

(21) 国際出願番号: PCT/JP2005/007254

(22) 国際出願日: 2005 年4 月14 日 (14.04.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-118740 2004 年4 月14 日 (14.04.2004) JP
特願2004-209367 2004 年7 月16 日 (16.07.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町二丁目３番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 松浦 克智 (MATSUURA, Katsunori) [JP/JP]; 〒1808585 東京都武蔵野市緑町三丁目９番１１号ＮＴＴ知的財産センタ内 Tokyo (JP).

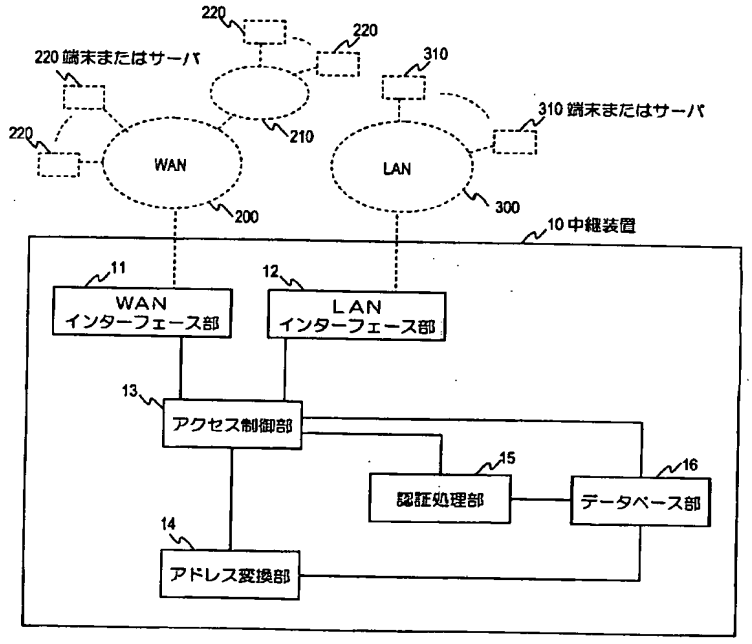
(74) 代理人: 草野 卓 (KUSANO, Takashi); 〒1600022 東京都新宿区新宿三丁目１番２２号 新宿ＮＳＯビル４階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ,

[続葉有]

(54) Title: ADDRESS CONVERSION METHOD, ACCESS CONTROL METHOD, AND DEVICE USING THESE METHODS

(54) 発明の名称: アドレス変換方法、アクセス制御方法、及びそれらの方法を用いた装置



220... TERMINAL OR SERVER
310... TERMINAL OR SERVER
10... RELAY DEVICE
11... WAN INTERFACE UNIT
12... LAN INTERFACE UNIT
13... ACCESS CONTROL UNIT
15... AUTHENTICATION UNIT
16... DATABASE UNIT
14... ADDRESS CONVERSION UNIT

(57) Abstract: According to the conventional address conversion technique, between terminals not compatible with encapsulation, only one terminal can be correlated to one port number and a plurality of terminal devices cannot be accessed by the same port number. In the present invention, according to an access control rule defined for each device of the packet transmission source or transmission source network, access from a global network to a private network is limited. Moreover, according to an address conversion rule defined for each transmission source device, address conversion is performed and communication is performed with the global network and the private network. Moreover, when a connection request is made by the global network and authentication is successful, an access control rule is defined for each transmission source device or each transmission source network and an address conversion rule is defined for each transmission source device and recorded. When the communication is complete, the access control rule and the address conversion rule are deleted.

(57) 要約: 従来のアドレス変換技術では、カプセル化に対応していない端末間では、１つのポート番号に１つの端末装置しか対応させることができず、同じポート番号で複数の端末装置へアクセスさせることができない。 本発明では、パケットの送信元の装置または送信元のネットワークごとに定

[続葉有]

WO 2005/101217 A1

NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書
— 補正書・説明書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

めたアクセス制御ルールに従って、グローバルネットワークからプライベートネットワークへのアクセスを制限する。また、送信元の装置ごとに定めたアドレス変換ルールに従って、アドレス変換を行って、グローバルネットワークとプライベートネットワークとの通信を行う。　また、グローバルネットワーク側からの接続要求があり、認証に合格した場合には、送信元の装置ごとまたは送信元のネットワークごとにアクセス制御ルールを定め、送信元の装置ごとにアドレス変換ルールを定めて記録する。通信が終了すると、追加したアクセス制御ルールとアドレス変換ルールとを削除する。

明 細 書

アドレス変換方法、アクセス制御方法、及びそれらの方法を用いた装置

技術分野

[0001] グローバルネットワークでのアドレスを持たないプライベートネットワークの端末が、前記グローバルネットワークを介して通信を行うためのアドレス変換技術及びアクセス制御技術(ファイアウォール技術)に関する。

背景技術

[0002] 従来より、グローバルネットワークとプライベートネットワークとの間、例えばインターネットなどの広域通信網(WAN:Wide Area Network)とイーサネット(登録商標)等のローカルエリアネットワーク(LAN)との間に配置され、WANからLAN内の端末装置へのパケットの宛先アドレスをグローバルIPアドレスからプライベートアドレスに変換し、LAN内の端末装置からWANへのパケットの送信元アドレスをプライベートアドレスからグローバルIPアドレスに変換することにより、LAN内のプライベートアドレスしか持たない複数の端末装置が1つのグローバルIPアドレスを共有してWANにアクセスできるようにするアドレス変換技術(NAT(Network Address Translation)技術)がある。また、LAN内の資源を保護するために、WANからのパケットの宛先や送信元をチェックし、設定されたセキュリティポリシーに従って許可されたパケットのみLAN内に通過させるアクセス制御技術(ファイアウォール技術)がある。そして、アドレス変換機能とアクセス制御機能を備えた中継装置、アドレス変換機能のみを備えたアドレス変換装置、アクセス制御機能のみを備えたファイアウォール装置が知られている。

[0003] 従来のアドレス変換技術では、インターネット側からのアクセスを、TCP(Transmission Control Protocol)またはUDP(User Datagram Protocol)のポート番号により端末装置に振り分けることにより、インターネットからLAN内の端末装置へのアクセスを可能にするものがある(例えば、特許文献1参照)。しかし、このようなインターネット側からのアクセスを、TCPまたはUDPのポート番号により端末装置に振り分けるアドレス変換装置では、インターネットからLAN内の端末装置へアクセスさせる時にTCPまたはUDPのポート番号を使っているので、1つのポート番号に1つの端末

装置しか対応させることができず、同じポート番号で複数の端末装置へアクセスさせることができない。例えばhttp(Hyper Text Transport Protocol)のデフォルトポート番号である80番で複数のサーバを公開できないという問題があった。また、TCPやUDPではないプロトコルで、ポート番号等が無い通信の場合(IPsec(Security Architecture for Internet Protocol)やICMP(Internet Control Message Protocol)等の場合)も、複数の端末装置を公開することができない、例えばIPsecのパケットは1つの端末装置へという設定しかできないため、複数の端末装置で同時にIPsecを使うことができない。これは、LAN内からインターネット側へ向けて通信する場合にも同じように起こるため、LAN内の端末装置でIPsecを利用することは困難である。 この問題を解決するため、IPsecのパケットをUDPのパケットにカプセル化して送るようにしたものもある(例えば、特許文献2参照)。しかし、このようなカプセル化を用いたアドレス変換技術では、IPsec通信を行う双方でUDPパケットへのカプセル化に対応している必要があり、UDPパケットへのカプセル化に対応していない端末とは通信することができなかった。

[0004] 一方、アクセス制御技術では、認証により確認された利用者からのアクセスにより、インターネットからでもファイアウォール装置に設定されているセキュリティポリシーを変更可能にしたものもある(例えば特許文献3参照)。この特許文献3に示す技術を、図1を参照して説明する。インターネット(WAN)200に接続された利用者端末220の利用者が、ファイアウォール装置900内のアクセス制御テーブル900a内のアクセス制御規則を変更したい場合は、利用者端末220から、LAN300に接続されている認証サーバ390に認証依頼をする。認証サーバ390のポート番号は、アクセス制御テーブル900aにどのパケットでも通過させる条件として記録されている。認証依頼には利用者のID(識別情報)と利用者の署名データ、実行したいアクセス内容として自己のIPアドレスやポート番号及びアクセスの相手先のIPアドレスやポート番号が含まれている。

[0005] 認証サーバ900は受信した認証依頼に対する検証を行い、検証に合格すれば、その認証依頼中の実行したいアクセス内容をアクセス制御テーブル900aに設定するように、ファイアウォール装置900に依頼する。従って、この依頼が例えば利用者端末2

20からLAN300に接続されたウェブ(Web)サーバ310に対するアクセスであれば、利用者は利用者端末220からWebサーバ310にアクセスして、例えばコンテンツをダウンロードすることが可能になる。このようにファイアウォール装置外からアクセス制御テーブル900aに設定されたアクセスの許可は、所定期間経過した場合又はアクセスが所定期間以上になると元に戻す。

特許文献1:特開2002－185517号公報

特許文献2:特開2002－232450号公報

特許文献3:特開2003－132020号公報

発明の開示

発明が解決しようとする課題

[0006] 従来のアドレス変換技術では、カプセル化に対応していない端末間では、1つのポート番号に1つの端末装置しか対応させることができず、同じポート番号で複数の端末装置へアクセスさせることができない。

また、従来のアクセス制御技術では、セキュリティポリシーを動的に変更できて便利である。しかし、その認証依頼を行った利用者装置またはその利用装置になりすました装置が、当初のアクセスの目的での通信が終了した後(例えばLAN内のWebサーバからのコンテンツダウンロードを終了した後)、所定期間通過可能に設定されていることを利用して、不正なアクセスをする恐れがある。この点で、セキュリティを確保することができないという問題があった。

[0007] 本発明では、アドレス変換技術に関しては、カプセル化に対応していない端末間でも、同じポート番号で複数のサーバを公開したり、ポート番号の無いプロトコルでも複数の通信を行ったりすることができるアドレス変換技術を提供することを目的とする。また、アクセス制御技術に関しては、セキュリティポリシー、つまり通過条件を動的に変えてもセキュリティを確保することのできるアクセス制御技術を提供することを目的とする。

課題を解決するための手段

[0008] 本発明は、グローバルネットワーク側の送信元の装置または送信元のネットワークごとに定めたアクセス制御ルールと、送信元の装置ごとに定めたアドレス変換ルールと

をデータベース部に記録しておく。グローバルネットワーク側からのパケットを受信すると、送信元情報を含んだアクセス制御ルールに従って、グローバルネットワークからプライベートネットワークへのアクセスを制限する。また、送信元情報を含んだアドレス変換ルールに従って、宛先アドレスの変換を行って、グローバルネットワーク側からの情報をプライベートネットワーク側に伝える。プライベートネットワーク側からのパケットを受信すると、送信元情報を含んだアドレス変換ルールに従って、送信元アドレスの変換を行って、プライベートネットワーク側からの情報をグローバルネットワーク側に伝える。

[0009] グローバルネットワーク側からのアクセス要求に対しては、データベース部に、通信を希望する宛先と送信元との間のアクセス制御ルールとアドレス変換ルールを追加・削除する場合には、認証を行う。認証に合格した場合には、送信元の装置ごとまたは送信元のネットワークごとにアクセス制御ルールを定め、送信元の装置ごとにアドレス変換ルールを定めてデータベース部に記録する。通信が終了すると、追加したアクセス制御ルールとアドレス変換ルールとをデータベース部から削除する。

プライベートネットワーク側からのアクセス要求に対しては、データベース部に通信を希望する宛先と送信元との間のアクセス制御ルールとアドレス変換ルールがない場合には、送信元ごとのアクセス制御ルールとアドレス変換ルールとを定めてデータベース部に記録する。通信が終了すると追加したアクセス制御ルールとアドレス変換ルールとをデータベース部から削除する。

[0010] 前記の認証については、中継装置内部の認証処理部で行う方法と、認証サーバをグローバルネットワーク内に設置し、中継装置へのアクセス制御ルール(ファイアウォール装置への通過条件設定)追加依頼は、認証サーバのみが行う方法とがある。

また、前記の方法をアドレス変換ルールのみに適用してアドレス変換方法とし、アクセス制御ルールのみに適用してファイアウォール方法とする。さらに、ファイアウォール技術に対しては、安全なセッションを確立中はそのセッションの通信状況をその安全なセッションにより要求元に通知する。

発明の効果

[0011] 本発明によれば、送信元アドレスが異なっているパケットには異なったアクセス制御

ルールとアドレス変換ルールとを適用させることができる。したがって、同じポート番号で、プライベートネットワークの複数のサーバを公開すること、及び、ポート番号の無いプロトコルで、プライベートネットワークの複数の端末が同時に通信を行うことができる。

プライベートネットワークの端末からのパケットを受信した場合は、該パケットに対するアクセス制御ルールとアドレス変換ルールとが登録されていなければ、該パケットに対するアクセス制御ルールとアドレス変換ルールとを追加する。したがって、プライベートネットワークの端末から開始される通信のアクセス制御ルールとアドレス変換ルールとを自動的に登録することができ、事前のアクセス制御ルール及びアドレス変換ルールの登録無しに通信を行うことができる。

[0012] アクセス制御技術に関しては、ファイアウォール装置外からファイアウォール装置の通過条件を動的に変更して、対応利用者端末からのパケットがファイアウォール装置を通過できるようにできる。しかもその安全なセッション切断時にはその通過許可(アクセス制御ルール)が解除される。したがって、そのセッション切断後の不正なパケットはファイアウォール装置を通過できない。また、確立しているセッションでの通信状況を要求元に通知する場合は、要求元で不正な通信を監視させることができる。

さらに、所定の認証サーバからの要求のみを受け付け、ファイアウォール装置の設定やアドレス変換ルールを変更する場合は、ポートスキャンにより、装置の存在やサービスの提供などを検知されることなく、グローバルなネットワークからアクセス制御やアドレス変換の設定を変更できる。

図面の簡単な説明

[0013] [図1]従来のファイアウォール装置を説明するためのシステム構成を示す図。

[図2]実施例1の中継装置の機能構成例を示す図。

[図3]実施例1でのアクセス制御テーブルの初期状態を示す図。

[図4]実施例1でのアドレス変換テーブルの初期状態を示す図。

[図5]実施例1の処理フローを示す図。

[図6]実施例1でのアクセス制御ルール追加後のアクセス制御テーブルを示す図。

[図7]実施例1でのアドレス変換ルール追加後のアドレス変換テーブルを示す図。

[図8]実施例2での、インターネットを介して通信可能な第1の中継装置と第2の中継装置、及びそれらに接続されたLANと端末の構成を示す図。

[図9]実施例2の処理フローを示す図。

[図10]実施例2で、第1の中継装置に追加するアクセス制御ルールを示す図。

[図11]実施例2で、第1の中継装置に追加するアドレス変換ルールを示す図。

[図12]実施例2で、第2の中継装置に追加するアドレス変換ルールを示す図。

[図13]実施例2で、第2の中継装置に追加するアクセス制御ルールを示す図。

[図14]実施例3のWAN上の認証サーバを用いた場合の中継装置の機能構成例を示す図。

[図15]実施例3でのアクセス制御テーブルの初期状態を示す図。

[図16]実施例3でのアドレス変換テーブルの初期状態を示す図。

[図17]実施例3のインターネット上の認証サーバと端末及びLAN上の端末やサーバとの構成を示す図。

[図18]実施例3の処理フローを示す図。

[図19]実施例3の認証サーバが追加を求めるアクセス制御ルールを示す図。

[図20]実施例3の認証サーバが追加を求めるアドレス変換ルールを示す図。

[図21]実施例3でのアクセス制御ルール追加後のアクセス制御テーブルを示す図。

[図22]実施例3でのアドレス変換ルール追加後のアドレス変換テーブルを示す図。

[図23]実施例4のアドレス変換装置の機能構成例を示す図。

[図24]実施例4のアドレス変換テーブルの初期状態を示す図。

[図25]実施例4のアドレス変換ルール追加後のアドレス変換テーブルを示す図。

[図26]実施例4のアドレス変換装置の通信開通までの処理フローを示す図。

[図27]実施例4のアドレス変換装置の通信開通後の処理フローを示す図。

[図28]ファイアウォール装置の機能構成例を示す図。

[図29]ファイアウォール装置の処理フローを示す図。

[図30]実施例5のアクセス制御テーブル(通過条件テーブル)の初期状態を示す図。

[図31]実施例5のアクセス制御ルール(通過条件)追加後のアクセス制御テーブル(通過条件テーブル)を示す図。

[図32]実施例6のアクセス制御ルール(通過条件)追加後のアクセス制御テーブル(通過条件テーブル)を示す図。

[図33]実施例7のアクセス制御ルール(通過条件)追加後のアクセス制御テーブル(通過条件テーブル)を示す図。

[図34]実施例8のファイアウォール装置の処理フローを示す図。

発明を実施するための最良の形態

[0014] 以下にこの発明の実施例を、図面を参照して説明するが、各図中の同一の構成要素には同一参照番号を付けて重複説明を省略する。

[実施例1]

図2は実施例1の中継装置10の機能構成例を示す図である。

図2において、本実施例の中継装置10は、インターネットなどの広域通信網(WAN(Wide Area Network))200とのパケットの送受信を行うWANインターフェース部11と、LAN300とのパケットの送受信を行うLANインターフェース部12と、WANインターフェース部11及びLANインターフェース部12が受信したパケットを分析してアクセス制御を行うアクセス制御部13と、アクセス制御部13で通過が許可されたパケット及びLAN内からWAN側へ送信されるパケットを分析してアドレス変換を行うアドレス変換部14と、アクセス制御部13の要求によりユーザの認証処理を行う認証処理部15と、アクセス制御のためのデータやアドレス変換のためのデータや認証のデータを蓄えているデータベース部16とを備えている。

[0015] この中継装置10は、アクセス制御機能(ファイアウォール機能)を備えており、アクセス制御部13は、データベース部16に記録されている図3に示すようなアクセス制御テーブルに基づいて、WANインターフェース部11で受信したパケットを、LANインターフェース部12を介してLAN側に送信するかを決定している。

図3において、「ソースIPアドレス」の列は、WANインターフェース部11で受信したパケットの送信元IPアドレスを示し、「プロトコル、ソースポート番号」の列は、WANインターフェース部11で受信したパケットのプロトコル名、及び該プロトコルでポート番号を使用する場合の送信元ポート番号を示し、「ディスティネーションIPアドレス」の列は、WANインターフェース部11で受信したパケットの宛先IPアドレスを示し、「プロ

トコル、ディスティネーションポート番号」の列は、WANインターフェース部11で受信したパケットのプロトコル名、及び該プロトコルでポート番号を使用する場合の宛先ポート番号を示し、「動作」の列は、WANインターフェース部11で受信したパケットの送信元及び宛先が、当該行のそれぞれの値に一致したときに、そのパケットに対して行われる動作を示している。

[0016] なお、「プロトコル、ソースポート番号」及び「プロトコル、ディスティネーションポート番号」の列で使用されるプロトコル名として、あらかじめ設定されたプロトコル名とポート番号に対応付けられたプロトコル名を使用することができる。

例えば、図3の1行目は、送信元IPアドレス、ポート番号に関係なく、宛先IPアドレスが「111. 111. 111. 2」でかつプロトコル名が「http(HyperText Transport Protocol、例えばTCP(Transmission Control Protocol)80)」であるパケットは、LAN側に送信されることを示している(通過:accept)。

[0017] 同様に、図3の2行目では、送信元IPアドレスが「123. 123. 123. 1」で、宛先IPアドレスが「111. 111. 111. 2」でかつプロトコル名が「SSH(Secure Shell、例えばTCP22)」であるパケットは、LAN側に送信され、3行目では、全てのパケットが廃棄される(廃棄:drop)。

アクセス制御部13は、このようなテーブルを上の行から、受信したパケットと一致するか検証し、一致すれば指定された動作を行い、そのパケットに対する処理は終了する。すなわち、図3のテーブルでは、上の行に設定された条件がより優先的に処理される条件となっている。

[0018] 中継装置10は、データベース部16に、図4に示すようなアドレス変換テーブルを記録している。アドレス変換部14は、WANインターフェース部11で受信し、アクセス制御部13を通過したパケットのディスティネーションIPアドレスを、このアドレス変換テーブルに基づいて、LANの内部のIPアドレスに変換して、LANインターフェース部12を介してLAN側に送信する。

また、LANインターフェース部12で受信したパケットのソースIPアドレスを、WANのIPアドレス(グローバルアドレス)に変換してアクセス制御部13に出力する。アクセス制御部13は、許可されたパケットを、WANインターフェース部11を介してWAN側

に送信する。

[0019] 図4において、「ソースIPアドレス」の列は、WANインターフェース部11で受信したパケットの送信元IPアドレスを示し、「ディスティネーションIPアドレス」の列は、WANインターフェース部11で受信したパケットの宛先IPアドレスを示し、「プロトコル、ディスティネーションポート番号」の列は、WANインターフェース部11で受信したパケットのプロトコル名及び該プロトコルでポート番号を使用する場合の宛先ポート番号を示し、「内部IPアドレス」の列は、WANインターフェース部11で受信したパケットの送信元及び宛先が、当該行のそれぞれの値に一致したときに、そのパケットの宛先IPアドレスに設定するLANのプライベートアドレスを示し、「プロトコル及びポート番号」の列は、WANインターフェース部11で受信したパケットの送信元及び宛先が、当該行のそれぞれの値に一致したときに、そのパケットの宛先ポート番号に設定するポート番号を示している。ただし、「any」の場合は任意のアドレスで良い。

[0020] 例えば、図4の1行目は、送信元IPアドレスに関係なく、宛先IPアドレスが「111. 111. 111. 2」でかつ宛先ポート番号が「TCP80(http)」であるパケットは、宛先IPアドレスを「192. 168. 100. 5」に書き替えられ、宛先ポート番号はそのままでLAN側に送信されることを示している。

図4の2行目は、送信元IPアドレスが「123. 123. 123. 1」で、宛先IPアドレスが「111. 111. 111. 2」でかつ宛先ポート番号が「TCP22(SSH)」であるパケットは、宛先IPアドレスを「192. 168. 100. 5」に書き替えられ、宛先ポート番号はそのままでLAN側に送信されることを示している。

[0021] このように設定することで、WAN側からの特定ポートへのアクセス、またはポートを持たないプロトコルへのアクセスを、LAN内の端末に振り分けることができる。

ここで、アドレス変換部14は、図4に示すようなアドレス変換テーブルを上の行から検索し、受信したパケットが一致すれば指定された動作を行い、そのパケットに対する処理は終了する。すなわち、図4のアドレス変換テーブルでは、上の行に設定された条件が、より優先的に処理される。

図4は、アドレス変換テーブルの初期状態(通信中の端末が無い状態)を示している。中継装置10は、LAN内の端末からの通信要求またはWAN側の端末からの要

求により、図3のアクセス制御テーブルにアクセス制御ルールを追加し、図4のアドレス変換テーブルにアドレス変換ルールを追加する。

[0022] 具体的には、図5を用いて説明する。アクセス制御部13は、自装置のグローバルアドレス宛のhttps(HyperText Transfer Protocol Security)のアクセス要求パケットを、WANインターフェース部11を介して受信すると(ステップS1)、送信元の端末とSSL(Secure Socket Layer)セッションの確立を行う(ステップS2)。セッションが正常に確立されれば、セッション確立時に取得した送信元端末のIPアドレスを記憶する(ステップS3)。次に、ユーザの認証を行うために、ユーザの識別情報とパスワードを入力させるHTMLファイルを暗号化して要求元の端末に、WANインターフェース部11を介して送信する(ステップS4)。

[0023] アクセス制御部13は、要求元の端末から、暗号化されたユーザの識別情報とパスワードを受信する(ステップS5)。次に、アクセス制御部13は、復号化を行い、ユーザの識別情報とパスワードを認証処理部15に送信し、ユーザの認証を要求する。

認証処理部15は、ユーザの識別情報とパスワードを受信すると、データベース部16に蓄積しているユーザの情報から、受信したユーザ識別情報と一致する識別情報を持つユーザを検索する。一致するユーザが見つかれば、蓄積しているそのユーザのパスワードと受信したパスワードを比較する(ステップS6)。認証処理部15は、パスワードが一致していれば、認証が正常であることをアクセス制御部13に送信する。一致するユーザが見つからない場合またはパスワードが一致しない場合は、認証異常をアクセス制御部13に送信する(ステップS7)。

[0024] アクセス制御部13は、認証処理部15から認証正常を受信すると、アクセスしたいサーバのLAN内部のプライベートアドレスやプロトコルやポート番号などを入力させるHTMLファイルを、暗号化して、要求元の端末に、WANインターフェース部11を介して送信する(ステップS9)。

アクセス制御部13は、要求元の端末から、暗号化されたプライベートアドレスやプロトコルやポート番号を受信する(ステップS10)。次に、アクセス制御部13は、復号化を行い、記憶しているhttpsのアクセス要求パケットの送信元IPアドレスを「ソースIPアドレス」、受信したプロトコル、ポート番号を「プロトコル、ディスティネーションポート

番号」としたアクセス制御ルールを、データベース部16のアクセス制御テーブルに追加する(ステップS11)。また、アクセス制御部13は、アドレス変換部14に、httpsのアクセス要求パケットの送信元IPアドレス、受信したプライベートアドレス、プロトコル、ポート番号を送り、アドレス変換ルールの追加を要求する。アドレス変換部14は、アドレス変換ルールの追加要求を受けると、httpsのアクセス要求パケットの送信元IPアドレスを「ソースIPアドレス」、受信したプライベートアドレスを「内部IPアドレス」、プロトコル、ポート番号を「プロトコル、ディスティネーションポート番号」としたアドレス変換ルールを、データベース部16のアドレス変換テーブルに追加する(ステップS12)。

[0025] 例えば、送信元IPアドレス「111. 222. 234. 123」の端末からのhttpsのアクセス要求パケットにより、宛先IPアドレス「111. 111. 111. 2」、宛先ポート番号「TCP22」のパケットの宛先IPアドレスを、内部IPアドレス「192. 168. 100. 4」に書き替えるようにする場合、アクセス制御テーブルは、図6に示すように、図3のテーブルの一番上の行に、httpsによりアクセスしてきた端末のアクセス制御ルールを追加する。また、アドレス変換テーブルは、図7に示すように、図4のテーブルの一番上の行に、httpsによりアクセスしてきた端末のアドレス変換ルールを追加する。

[0026] これにより、送信元IPアドレス「111. 222. 234. 123」、宛先IPアドレス「111. 111. 111. 2」、宛先ポート番号「TCP22」のパケットは、アクセス制御部13を通過する。また、アドレス変換部14で宛先IPアドレスを192. 168. 100. 4に書き替えられてLANに送信される。それ以外の送信元IPアドレスの宛先ポート番号が「TCP22」のパケットは、アクセス制御部13で廃棄される。

その後、アクセス制御部13は、認証が正常でアドレス変換が設定された旨と、変換先のLAN内部のプライベートアドレスとプロトコルとポート番号などを表示するHTMLファイルを、暗号化して、端末に送信する(ステップS13)。なお、このHTMLファイルには、端末があらかじめ定めた一定時間ごとに、中継装置10にアクセスするためのプログラムが埋め込まれている。

[0027] 端末では、送信されたHTMLファイルを復号化して表示することにより、設定されたアドレス変換の情報を確認することができる。また、HTMLファイルに埋め込まれたプログラムにより、端末は一定時間ごとに、中継装置10に信号を送りはじめる。

このようにしてアクセス制御ルール及びアドレス変換ルールを設定し、LAN内の端末との通信を行う。ユーザが通信を終了するときは、中継装置10から受信したHTMLファイルで表示された画面から、通信の終了のボタンを選択するか、HTMLファイルを表示しているブラウザを閉じるか、HTMLファイルを表示している端末を終了(電源オフ、ログオフ等)する。

[0028] 中継装置10のアクセス制御部13は、通信終了のパケットを受信した場合、端末からの信号が一定時間送信されてこないことによりブラウザが閉じられたことや端末が終了されたことを検出した場合(ステップS14)、図6のように書き替えたテーブルを、図3のような元の状態に戻し、アドレス変換部14にソースIPアドレス、ディスティネーションIPアドレス、プロトコルを送信し、この通信が終了したことを通知する(ステップS15)。アドレス変換部14は、通信の終了の通知を受けると、図7のように書き替えたテーブルを、図4のような元の状態に戻す(ステップS16)。

[0029] 上記のように、本実施例では、ソースIPアドレスを使用したアクセス制御ルールとアドレス変換ルールを、アクセス制御テーブルとアドレス変換テーブルに設定する。したがって、宛先が同じポート番号の場合でも、ソースIPアドレスにより別々のサーバへ振り分けたり、ポート番号の無いプロトコルでもソースIPアドレスにより別々の端末と通信を行わせたりすることができる。

なお、本実施例では、httpsのアクセスによりアドレス変換ルール、アクセス制御ルールの追加を受け付けるようにしたが、httpやSIP(Session Initiation Protocol)やSSHやtelnetなどを使ってもよい。

[0030] [実施例2]

実施例1に示した中継装置10は、LAN(プライベートネットワーク)内の端末からIPsec通信の最初のパケットを受信したときに、宛先IPアドレスと送信元IPアドレス(プライベートネットワーク側が送信元となる。)とのアドレス変換ルールをアドレス変換テーブルに追加することで、LAN内の複数の端末が中継装置10を通してIPsec通信を行うことができる。図8にインターネットを介して通信可能な第1の中継装置10aと第2の中継装置10b、及びそれらに接続されたLANと端末の構成を示す。以下に、LAN300の端末とLAN400の端末間でのIPsec通信の場合について、図9を用いて説

明する。

[0031] まず、端末410aは、LAN300内の端末310aとのIPsec通信に必要なアドレス変換ルールを、第1の中継装置10aに追加するため、第1の中継装置10aにhttpsのアクセス要求パケットを送信する。

第1の中継装置10aは、httpsのアクセス要求パケットを受信すると、送信元の端末とSSLセッションの確立を行い(ステップS21)、ユーザの認証を行い(ステップS22)、認証されれば、アクセスしたいサーバのLAN内部のプライベートアドレスやプロトコルやポート番号などを入力させるHTMLファイルを要求元の端末410aに送信する。なお、このHTMLファイルには、端末があらかじめ定めた一定時間ごとに、中継装置10aにアクセスするためのプログラムが埋め込まれている。

[0032] 端末410aは、受信したHTMLファイルを表示して(ステップS23)、利用者にアクセス先の情報を入力させる。この場合、接続したい端末310aのプライベートIPアドレス192. 168. 100. 2と、プロトコルとしてIPsecが入力される。端末410aは、入力されたプライベートアドレスとプロトコルを第1の中継装置 10aに送信する。

第1の中継装置10aは、プライベートアドレスとプロトコルを受信すると、データベース部16に記録しているhttpsのアクセス要求パケットの送信元IPアドレス(第2の中継装置10bのIPアドレス111. 222. 234. 123)を「ソースIPアドレス」、IPsecを「プロトコル、ソースポート番号」、自装置のグローバルアドレス211. 250. 250. 100を「ディスティネーションIPアドレス」、IPsecを「プロトコル、ディスティネーションポート番号」とした図10に示すアクセス制御ルールを追加する。また、httpsのアクセス要求パケットの送信元IPアドレスを「ソースIPアドレス」、自装置のグローバルアドレス211. 250. 250. 100を「ディスティネーションIPアドレス」、IPsecを「プロトコル、ディスティネーションポート番号」、192. 168. 100. 2を「内部IPアドレス」とした図11に示すアドレス変換ルールを追加する(ステップS24)。

[0033] 端末410aが、最初のIPsecパケットを第2の中継装置10bに送信すると、第2の中継装置10bのアドレス変換部14は、IPsec通信に関するアドレス変換ルールがアドレス変換テーブルに登録されているかを調べる。具体的には、パケットの宛先IPアドレスとアドレス変換テーブルのソースIPアドレス、パケットの送信元IPアドレスとアドレス

変換テーブルと内部IPアドレスとが一致するアドレス変換ルールが有るかを検索する(ステップS26)。

この条件に合致するアドレス変換ルールがあれば、送信元IPアドレスをそのアドレス変換ルールのディスティネーションIPアドレスのアドレスに書き換え(ステップS27)、書き換えたパケットを、アクセス制御部13を通して送信する。

[0034] この条件に合致するアドレス変換ルールが無ければ、宛先IPアドレスを「ソースIPアドレス」、自装置のIPアドレス(この場合、111. 222. 234. 123)を「ディスティネーションIPアドレス」、IPsecを「プロトコル、ディスティネーションポート番号」、送信元IPアドレス(この場合、192. 168. 20. 2)を「内部IPアドレス」とした図12に示すアドレス変換ルールを追加する。また、アクセス制御部13に、送信元IPアドレスが211. 250. 250. 100で、宛先IPアドレスが111. 222. 234. 123のIPsecパケットの通過を許可するアクセス制御ルールの追加を要求する。アクセス制御部13は、図13に示すアクセス制御ルールを追加する。

[0035] アドレス変換部14は、アクセス制御部13のアクセス制御ルールの追加が終わると、受信したパケットの送信元IPアドレスを自装置のグローバルIPアドレス(この場合、111. 222. 234. 123)に書き換え、書き換えたパケットをアクセス制御部13経由で送信する。以降、端末310aと端末410aとの間でIPsecによる通信が行われる。

IPsecによる通信が終了すると、端末410aの利用者が、第1の中継装置10aから受信したHTMLファイルで表示された画面から、通信終了のボタンを選択するか、HTMLファイルを表示しているブラウザを閉じるか、HTMLファイルを表示している端末を終了する(ステップS30)。

[0036] 第1の中継装置10aのアクセス制御部13は、通信終了のパケットの受信、端末410aからの信号が一定時間送信されてこないことによりブラウザが閉じられたこと、もしくは端末が終了されたことを検出すると(ステップS31)、図10に示したアクセス制御ルールを削除する。また、アドレス変換部14にソースIPアドレス111. 222. 234. 123、ディスティネーションIPアドレス211. 250. 250. 100、プロトコルIPsecの通信が終了したことを通知する。アドレス変換部14は、通信の終了の通知を受けると、図11に示したアドレス変換ルールを削除する(ステップS32)。

[0037] 第2の中継装置10bのアクセス制御部13は、通信終了のパケットの受信、端末410aからの信号が一定時間送信されてこないことによりブラウザが閉じられたこと、もしくは端末が終了されたことを検出すると(ステップS33)、図13に示したアクセス制御ルールを削除する。また、アドレス変換部14にソースIPアドレス211. 250. 250. 100、ディスティネーションIPアドレス111. 222. 234. 123、プロトコルIPsecの通信が終了したことを通知する。アドレス変換部14は、通信の終了の通知を受けると、図12に示したアドレス変換ルールを削除する(ステップS34)。

[0038] 上記のように、本実施例では、ソースIPアドレスを使用したアクセス制御ルールとアドレス変換ルールを、アクセス制御テーブルとアドレス変換テーブルにそれぞれ設定する。したがって、宛先が同じポート番号の場合でもソースIPアドレスごとに別々のサーバへ振り分けたり、ポート番号の無いプロトコルの場合でもソースIPアドレスごとに別々の端末と通信を行わせたりすることができる。

また、LAN側から受信したIPsecのパケットの宛先IPアドレスと送信元IPアドレスに対するアドレス変換ルールが登録されていない場合でも、LAN内の端末から開始されるIPsec通信のアドレス変換ルールは、自動的に登録できるので、事前にアドレス変換ルールを登録すること無く、IPsec通信を行うことができる。

なお、本実施例では、IPsec通信の最初のパケットによりアドレス変換ルール、アクセス制御ルールを追加したが、IKE(Internet Key Exchange)の最初のパケットなどによりアドレス変換ルール、アクセス制御ルールを追加してもよい。

[0039] [実施例3]

実施例1と実施例2では、WAN側の端末の認証を中継装置10内の認証処理部15で行ったが、WAN上の認証サーバを経由させ、該認証サーバで認証を行わせ、該認証サーバからの要求によりアクセス制御ルール及びアドレス変換ルールを追加、削除してもよい。このようにすることにより、WAN上からステルス(アクセス可能なプロトコルやポート番号を隠蔽して)で運用することができる。

[0040] 図14はWAN上の認証サーバを用いた場合の中継装置の機能構成例を示す図である。図14の中継装置20は、インターネットなどの広域通信網(WAN)に接続され、WANとのパケットの送受信を行うWANインターフェース部11と、LANとのパケット

の送受信を行うLANインターフェース部12と、WANインターフェース部11及びLANインターフェース部12が受信したパケットを分析しアクセス制御を行うアクセス制御部23と、WAN側からLAN内へのパケットの宛先アドレス、及びLAN内からWAN側へのパケットの送信元アドレスを変換するアドレス変換部24と、アクセス制御のためのデータやアドレス変換のためのデータを蓄えているデータベース部26とを備えている。また、WAN上にはWAN側の端末の認証を行い、中継装置20にアクセス制御ルールの追加などを要求する認証サーバ100がある。認証サーバ100は、WAN側の端末及び中継装置20と通信を行うインターフェース部101、認証サーバ100の制御を行う制御部102、認証処理を行う認証処理部105、認証情報や通信中の情報などを記録するデータベース部106から構成されている。

[0041] 中継装置20は、ファイアウォール機能を備えている。具体的には、アクセス制御部23は、データベース部26に記録されている図15に示すアクセス制御テーブルに基づいて、WAN側から受信したパケットをLAN内に送信するかを決定している。

図15において、「ソースIPアドレス」の列は、WANインターフェース部11で受信したパケットの送信元IPアドレスを示し、「ソースポート番号」の列は、WANインターフェース部11で受信したパケットの送信元ポート番号を示し、「ディスティネーションIPアドレス」の列は、WANインターフェース部11で受信したパケットの宛先IPアドレスを示し、「プロトコル、ディスティネーションポート番号」の列は、WANインターフェース部11で受信したパケットのプロトコル名及び該プロトコルでポート番号を使用する場合の宛先ポート番号を示し、「動作」の列は、WANインターフェース部11で受信したパケットの送信元及び宛先が、当該行のそれぞれの値に一致したときに、そのパケットに対して行われる動作を示している。

[0042] なお、「プロトコル、ディスティネーションポート番号」の列で使用されるプロトコル名として、あらかじめ設定されてたプロトコル名とポート番号に対応付けられたプロトコル名を使用することができる。

例えば、図15の1行目では、送信元IPアドレス、ポート番号に関係なく、宛先IPアドレスが「123. 123. 123. 123」で、かつプロトコル名が「https(HyperText Transfer Protocol Security、例えばTCP443)」であるパケットは、LAN側に送信される(通過

:accept)。

[0043] 同様に、図15の2行目では、送信元IPアドレスが「211. 250. 250. 100」で、宛先IPアドレスが「123. 123. 123. 123」で、かつプロトコル名が「SSH(Secure Shell、例えばTCP22)」であるパケットは、LAN側に送信され、3行目では、全てのパケットが廃棄される(drop)。

アクセス制御部23は、このようなテーブルを上の行から受信したパケットが一致するか検証し、一致すれば指定された動作を行い、そのパケットに対する処理は終了する。すなわち、図15のテーブルでは、上の行に設定された条件がより優先的に処理される条件となっている。

[0044] また、中継装置20は、データベース部26に、図16に示すアドレス変換テーブルを記録しており、アドレス変換部24は、このテーブルに基づいて、WAN側から受信したパケットのディスティネーションIPアドレスをLANの内部のIPアドレスに変換して、LAN内に送信する。また、LAN側から受信したパケットのソースIPアドレスをWANのIPアドレス(グローバルアドレス)に変換して、WAN側に送信する。

図16において、「ソースIPアドレス」の列は、WANインターフェース部11で受信したパケットの送信元IPアドレスを示し、「ディスティネーションIPアドレス」の列は、WANインターフェース部11で受信したパケットの宛先IPアドレスを示し、「プロトコル、ディスティネーションポート番号」の列は、WANインターフェース部11で受信したパケットのプロトコル名及び該プロトコルでポート番号を使用する場合の宛先ポート番号を示し、「内部IPアドレス」の列は、WANインターフェース部11で受信したパケットの送信元及び宛先が、当該行のそれぞれの値に一致したときに、そのパケットの宛先IPアドレスに設定するLANのプライベートアドレスを示し、「プロトコル及びポート番号」の列は、WANインターフェース部11で受信したパケットの送信元及び宛先が、当該行のそれぞれの値に一致したときに、そのパケットの宛先ポート番号に設定するポート番号を示している。

[0045] 例えば、図16の1行目では、送信元IPアドレスに関係なく、宛先IPアドレスが「123. 123. 123. 123」でかつ宛先ポート番号が「TCP443(https)」であるパケットは、宛先IPアドレスを「192. 168. 100. 5」に書き替えられ、宛先ポート番号はそのまま

でLAN側に送信される。

同様に、図16の2行目では、送信元IPアドレスが「211. 250. 250. 100」で、宛先IPアドレスが「123. 123. 123. 123」でかつ宛先ポート番号が「TCP22(SSH)」であるパケットは、宛先IPアドレスを「192. 168. 100. 5」に書き替えられ、宛先ポート番号はそのままでLAN側に送信される。

[0046] このように設定することで、WAN側からの特定ポートへのアクセス、またはポートを持たないプロトコルへのアクセスを、LAN内の端末に振り分けることができる。

また、アドレス変換部24は、このようなテーブルを上の行から受信したパケットが一致するか検証し、一致すれば指定された動作を行い、そのパケットに対する処理は終了する。すなわち、図16のテーブルでは、上の行に設定された条件がより優先的に処理される条件となっている。

また、図16に示した状態は、初期状態(通信中の端末が無い状態)である。LAN内の端末からの通信要求により、また後述するWAN側のサーバからの要求により、アドレス変換ルールが追加されて、LAN内からWAN側へのパケット、WAN側からLAN内へのパケットのそれぞれのアドレスが図16のテーブルに従って変換され、送信される。

[0047] 図17にインターネット上の認証サーバと端末及びLAN上の端末やサーバとの構成を示す。中継装置20は、LAN300に接続され、LAN300には端末310a, 310b及びサーバ311a, 311bが接続されている。中継装置20は、インターネット200上の認証サーバ100からの要求のみにより、図15のアクセス制御テーブルにアクセス制御ルールを追加し、図16のアドレス変換テーブルにアドレス変換ルールを追加できる。

認証サーバ100は、中継装置20にアクセス可能なユーザを認証するための認証情報や、ユーザごとにアクセスが許可されている中継装置20のアドレス、追加するアクセス制御ルール及びアドレス変換ルールなどのアクセス情報をデータベース部106に記録している。認証サーバ100は、インターネット200上の端末からの要求があると、データベース部106に記録した認証情報に基づいてユーザの認証を行い、認証が正常ならば中継装置にアクセス制御ルール及びアドレス変換ルールの追加を要求する。

[0048] 例えば、インターネット200上の端末220aとサーバ311aとの間で通信したい場合について、図18を用いて説明する。端末220aを操作するユーザは、インターネット200上の認証サーバ100に接続し、認証を受ける。この認証は、識別情報(ID)とパスワードの簡易なものから、ワンタイムパスワードや生体情報による高度なソフトウェア機能による認証でもよい。なお、このような認証に用いる情報は、インターネット上での情報漏洩を防ぐため、暗号化して送信することが好ましい。

認証サーバ100は、認証要求を受けると、認証要求した端末220aのアドレスを送信元アドレスとして記憶し(ステップS41)、認証情報に基づいてユーザの認証を行う(ステップS42)。

[0049] ユーザが認証されれば(ステップS43)、認証サーバ100は、記録している端末220aのアドレスを送信元アドレスとするアクセス制御ルールとアドレス変換ルールの追加を、中継装置20に要求する。例えば、端末220aからサーバ311aへのhttpアクセスのみ許可する場合、認証サーバ100は、図19に示す端末220aのアドレス(111. 222. 234. 123)を送信元としてhttpアクセスを許可するアクセス制御ルールの追加と、図20に示す端末220aのアドレス(111. 222. 234. 123)が送信元のhttpのパケットの送信先を、サーバ311aのアドレス(192. 168. 100. 4)に変更するアドレス変換ルールの追加とを、要求する。

[0050] 中継装置20のアクセス制御部23は、認証サーバ100からのアクセス制御ルールの追加要求及びアドレス変換ルールの追加要求を受信すると、受信したアクセス制御ルールをデータベース部26のアクセス制御テーブルに追加する。また、アクセス制御部23は、認証サーバ100から受信したアドレス変換ルールを追加するように、アドレス変換部24に要求する。アドレス変換部24は、アクセス制御部23からアドレス変換ルールの追加要求を受けると、受信したアドレス変換ルールをデータベース部26のアドレス変換テーブルに追加する(ステップS44)。例えば、上述の端末220aからサーバ311aへのhttpアクセスを許可する場合、図15のアクセス制御テーブルに図19のアクセス制御ルールを追加し、アクセス制御テーブルを図21のようにする。また、図16のアドレス変換テーブルに図20のアドレス変換ルールを追加し、アドレス変換テーブルを図22のようにする。

[0051] アクセス制御ルール及びアドレス変換ルールの追加が終わると、アクセス制御部23は、認証サーバ100に追加完了を返送する。

認証サーバ100は、中継装置20から追加完了を受信すると、記憶している端末220aのアドレス、中継装置20のアドレス、追加したアクセス制御ルール及びアドレス変換ルールを関連付けて通信中情報として記憶する(ステップS45)。また、認証サーバ100は、端末220aに対して、アクセスが可能になった旨と、アクセスが許可されたサービス名(例えば、Webカメラなど、IPアドレスとポート番号でもよい)などを、アクセス可能情報として送信する。

[0052] 端末220aでは、受信した情報を表示することにより(ステップS46)、アクセスが可能になった旨とアクセス可能情報をユーザに知らせる。

このようにして、端末220aからのhttpアクセスは、サーバ311aに振り分けられ、その他の端末からのhttpアクセスは拒否されることになる。アクセスが可能になったことを知ったユーザは、LAN300内の端末やサーバと通信を開始する。

LAN300内の端末やサーバとの通信を行ったユーザが、通信を終了するときは、端末220aから終了情報を入力し(ステップS51)、認証サーバ100に通信終了を通知する。

[0053] 認証サーバ100は、通信終了通知を受信すると、通信終了通知の送信元のアドレスから、通信中情報の端末側のアドレスに一致するものがあるか検索する(ステップS52)。通信中情報に一致するものがあれば(ステップS53)、関連付けられている中継装置20に、関連付けられているアクセス制御ルールとアドレス変換ルールの削除を要求する。

中継装置20のアクセス制御部23は、アクセス制御ルールとアドレス変換ルールの削除要求を受信すると、受信したアクセス制御ルールをデータベース部26のアクセス制御テーブルから削除する。また、アクセス制御部23は、認証サーバ100から受信したアドレス変換ルールを削除するように、アドレス変換部24に要求する。アドレス変換部24は、アクセス制御部23からアドレス変換ルールの削除要求を受けると、該当するアドレス変換ルールをデータベース部26のアドレス変換テーブルから削除する(ステップS54)。

[0054] このようにして、ユーザからの通信終了通知により、中継装置20のアクセス制御テーブルが図15のように戻され、アドレス変換テーブルが図16のように戻される。したがって、追加されたアクセス制御ルール及びアドレス変換ルールを利用した不正なアクセスを防止することができる。

また、中継装置20は、アクセス制御ルールとアドレス変換ルールの追加や削除の要求を認証サーバ100からのみ受け付ければよく、ポートスキャンによりポートを検知されること無くアクセス制御ルールとアドレス変換ルールを変更することができる。

[0055] さらに、認証サーバ100で認証を行っているので、IDとパスワードによる認証から、より高度な認証まで容易に行うことができる。

なお、端末220aからの通信終了の通知により、アクセス制御ルールとアドレス変換ルールを削除したが、パケットの送受信が一定時間以上無くなったときや、通信開始時から一定時間経過したときに通信終了と判断して、アクセス制御ルールとアドレス変換ルールを削除するようにしてもよい。

また、認証サーバ100にhttpサーバとしての機能を持たせ、認証の受付やアクセス可能情報の表示や通信終了の通知などを、ホームページ上で行えるようにしてもよい。また、認証サーバ100としてSIP(Session Initiation Protocol)サーバを用いてもよい。

また、アクセス制御ルールを、すべてのアクセスに対して通過と設定することで、アドレス変換装置として機能させることもできる。

[0056] [実施例4]

実施例1から3では、アクセス制御技術とアドレス変換技術とを用いて、中継装置の機能構成と処理フローについて示した。本実施例では、アドレス変換技術のみを用いて、アドレス変換装置と処理フローについて示す。図23は、アドレス変換装置の機能構成例を示すものである。アドレス変換装置30は、WANインターフェース部11、LANインターフェース部12、データベース部33、アドレス変換部34、認証処理部35から構成されている。

[0057] データベース部33は、アドレス変換テーブルを含むアドレス変換のためのデータ、ユーザ認証のためのデータ等を蓄積している。

図24にアドレス変換テーブルの一例を示す。また、図25は、図24のアドレス変換テーブルに、後述する送信元IPアドレスをソースIPアドレスとして含むアドレス変換ルールが追加された後のアドレス変換テーブルの一例を示すものである。

図24、図25において、「ソースIPアドレス」の列は、WANインターフェース部11で受信したパケットの送信元IPアドレスを示している(ただし、「any」の場合は任意のアドレスで良い。)。また、「ディスティネーションIPアドレス」の列は、WANインターフェース部11で受信したパケットの宛先IPアドレスを示している。また、「プロトコル、ディスティネーションポート番号」の列は、WANインターフェース部11で受信したパケットのプロトコル及び宛先ポート番号を示している。また、「内部IPアドレス」の列は、WANインターフェース部11で受信したパケットの送信元及び宛先が、当該行のそれぞれの値に一致した時に、そのパケットの宛先IPアドレスに設定するLAN内のプライベートアドレスを示している。また、「プロトコル及びポート番号」の列は、WANインターフェース部11で受信したパケットの送信元及び宛先が、当該行のそれぞれの値に一致した時に、そのパケットの宛先ポート番号に設定するポート番号を示している。 アドレス変換部34は、アドレス変換テーブルに対するアドレス変換ルールの追加と削除を行うとともに、該アドレス変換テーブルに基づいてWANインターフェース部11及びLANインターフェース部12で受信したパケットのアドレス変換を行う。

[0058] すなわち、アドレス変換部34は、WANインターフェース部11で受信したパケットについては、送信元IPアドレスと宛先IPアドレスにより前記アドレス変換テーブルを参照し、宛先IPアドレスをLAN内のIPアドレス(内部IPアドレス)に変換し、LANインターフェース部12を介してLAN側に送信する。

例えば、図24の1行目では、送信元IPアドレスに関係なく、宛先IPアドレスが「123.123.123.123」でかつ宛先ポート番号が「TCP443(https)」であるパケットは、宛先IPアドレスが「192.168.100.5」に書き替えられ、宛先ポート番号はそのままでLAN側に送信される。

[0059] 同様に、図24の2行目では、送信元IPアドレスに関係なく、宛先IPアドレスが「123.123.123.123」でかつ宛先ポート番号が「TCP22(SSH)」であるパケットは、宛先IPアドレスが「192.168.100.5」に書き替えられ、宛先ポート番号はそのままで

LAN側に送信される。

また、アドレス変換部34は、LANインターフェース部12で受信したパケットについては、パケットの宛先IPアドレスをソースIPアドレスと読み替えた上で、パケットの送信元IPアドレスと同じ内部IPアドレスをアドレス変換テーブル内で検索し、パケットの送信元IPアドレスをWAN内のグローバルIPアドレスに変換し、WANインターフェース部11を介してWAN側に送信する。

[0060] アドレス変換部34では、前述したアドレス変換テーブルを上の行から受信したパケットの内容により参照し、一致すれば指定された動作を行い、そのパケットに対する処理は終了する。即ち、図24、図25のアドレス変換テーブルでは、上の行に設定された条件がより優先的に処理される条件となっている。

認証処理部35は、アドレス変換部34の要求により、ユーザの認証処理を行う。

図26、図27はアドレス変換装置の処理フローを示すフローチャートであり、以下、これに従って本アドレス変換装置の動作を詳細に説明する。

[0061] アドレス変換部34は、WAN側の端末装置220からWANインターフェース部11を介して自装置のアドレス宛のhttpのアクセス要求(通信の開始要求)パケットを受信する(ステップS61)と、アクセス要求パケットの送信元IPアドレスを送信元の端末装置のIPアドレスとして記憶し(ステップS62)、ユーザの認証に必要なユーザの識別情報及びパスワードを入力させるためのHTML(Hyper Text Markup Language)ファイルを、アクセス要求元の端末装置220にWANインターフェース部11を介して送信する(ステップS63)。

[0062] アドレス変換部34は、アクセス要求元の端末装置220からユーザの識別情報及びパスワードを受信する(ステップS64)と、受信したユーザの識別情報及びパスワードを認証処理部35に転送し、ユーザの認証を要求する(ステップS65)。

認証処理部35は、ユーザの識別情報及びパスワードを受信すると、データベース部33に蓄積しているユーザの情報から、受信したユーザ識別情報と一致する識別情報を持つユーザを検索する。一致するユーザが見つかれば、蓄積しているそのユーザのパスワードと受信したパスワードを比較し、一致していれば、認証正常をアドレス変換部34に送信する(ステップS66)。一致するユーザが見つからなかった場合とパ

スワードが一致しなかった場合は、認証異常をアドレス変換部34に送信する。なお、この際、ユーザに再度、ユーザの識別情報やパスワードの入力を求め、所定の回数繰り返しても一致しない場合に認証異常とするようにしても良い。

[0063] アドレス変換部34は、認証処理部35から認証正常を受信すると、アクセスしたいサーバのLAN内部におけるプライベートアドレスやプロトコル、ポート番号等を入力させるためのHTMLファイルをアクセス要求元の端末装置220にWANインターフェース部11を介して送信する(ステップS67)。

アクセス要求元の端末装置220からプライベートアドレスやプロトコル、ポート番号等を受信する(ステップS68)と、アドレス変換部34は、記録しているhttpのアクセス要求パケットの送信元IPアドレスをソースIPアドレス、受信したプライベートアドレスを内部IPアドレス、プロトコル及びポート番号をプロトコル及びディスティネーションポート番号としたアドレス変換ルールを、データベース部33のアドレス変換テーブルに追加する(ステップS69)。

[0064] 例えば、httpのアクセス要求パケットの送信元IPアドレスが「111. 222. 234. 123」、宛先IPアドレスが「123. 123. 123. 123」、宛先ポート番号が「TCP22」のパケットの宛先IPアドレスを、内部IPアドレス「192. 168. 100. 4」に書き替えるようにする場合、図25に示すように、図24のテーブルの一番上の行に、httpによりアクセスしてきた端末のアドレス変換ルールを追加する。

これにより、送信元IPアドレスが「111. 222. 234. 123」、宛先ポート番号が「TCP22」のパケットは、宛先IPアドレスが「192. 168. 100. 4」に書き替えられてLANに送信され、それ以外の送信元IPアドレスの宛先ポート番号が「TCP22」のパケットは、宛先IPアドレスが「192. 168. 100. 5」に書き替えられてLANに送信されるようになる。

[0065] その後、アドレス変換部34は、アクセス要求元の端末装置220に対して、認証が正常であったこと、アドレス変換ルールが設定されたこと、変換先のLAN内部のプライベートアドレス、プロトコルとポート番号等を表示するHTMLファイルを送信する(ステップS70)。なお、このHTMLファイルには、端末があらかじめ定めた一定時間ごとに、中継装置10aにアクセスするためのプログラムが埋め込まれている。

アクセス要求元の端末装置220では、送信されたHTMLファイルを表示することにより、設定されたアドレス変換の情報を確認することができる。また、この後、端末装置220は、HTMLファイル内に埋め込まれたスクリプトなどのプログラムにより、一定時間ごとに自動的に、アドレス変換装置30へhttp通信を行う。

[0066] アドレス変換ルールの設定後、アドレス変換部34は、WANインターフェース部11からパケットを受信する(ステップS72, ステップS74)と、その送信元IPアドレス及び宛先IPアドレスにより前記アドレス変換テーブルを参照し(ステップS75)、宛先IPアドレスをLAN内のIPアドレス(内部IPアドレス)に変換し(ステップS76)、LANインターフェース部12を介してLANに送信する。

また、アドレス変換部34は、LANインターフェース部12からパケットを受信する(ステップS72, ステップS74)と、その内部IPアドレスにより前記アドレス変換テーブルを参照する(ステップS77)。次に、アドレス変換部34は、パケットの送信元IPアドレスを、内部IPアドレスからWAN内のグローバルIPアドレスに変換し(ステップS78)、WANインターフェース部11を介してWANに送信する。

[0067] このようにしてLAN内のサーバ(端末装置)との通信を行う。また、端末装置220のユーザが通信を終了する場合は、アドレス変換装置30から受信したHTMLファイルの画面から、通信の終了のボタンを選択し、通信終了のパケットを送信するか、当該画面自体を閉じる。

アドレス変換装置30のアドレス変換部34は、アクセス要求元の端末装置220のHTML画面の終了により通信の切断を検出する(ステップS71)か、通信終了のパケットを受信する(ステップS73)と、図25のように書き替えられていたアドレス変換テーブルから、追加されていたアドレス変換ルールを削除し(ステップS79)、図24の初期状態に戻す。

[0068] このように、本実施例では、ソースIPアドレスを含んだ条件によりアドレス変換ルールを設定することができるので、同じポート番号へのパケットでもソースIPアドレスごとに別々のサーバへ振り分けたり、ポート番号の無いプロトコルでもソースIPアドレスごとに別々の端末と通信を行わせたりすることができる。

また、ユーザのリクエストにより、または通信の切断により、変更したアドレス変換ル

ールの設定を元に戻しているので、変更した設定による誤ったアクセスを防ぐことができる。

[0069] なお、本実施例では、端末からアドレス変換装置へのアクセスにhttpを使ったが、httpsやtelnetやSIP(Session Initiation Protocol)等を使ってもかまわない。また、本実施例では、ユーザの認証を行ったが、あらかじめ設定された端末からの要求に対しては認証要求を行わないようにしても良い。

[0070] [実施例5]

本実施例では、本発明のアクセス制御技術のみを用いた技術を示す。ファイアウォール装置の機能構成例とファイアウォール方法の手順例を、それぞれ図28と図29に示す。

この実施の形態のファイアウォール装置40は、インターネットなどの広域通信網(WAN:Wide Area Network)200に接続され、WAN200とのパケットの送受信を行うWANインターフェース部11と、LAN300とのパケットの送受信を行うLANインターフェース部12と、WANインターフェース部11及びLANインターフェース部12が受信したパケットを分析してアクセス制御を行うアクセス制御部46と、アクセス制御部46の要求により利用者(ユーザ)の認証処理を行う認証処理部47と、アクセス制御のためのデータや認証のデータを蓄えているデータベース部48とを備えている。

[0071] データベース部48のアクセス制御テーブル(通過条件テーブル)48aには、図30に示すようなテーブルが記憶されており、アクセス制御部46は、このテーブルに基づいて、WANインターフェース部11で受信したパケットを、LANインターフェース部12を介してLAN300側に転送するかを決定している。

図30において、「ソースIPアドレス」の列は、WANインターフェース部11で受信したパケットの送信元IPアドレスを示し、「ソースポート番号」の列は、WANインターフェース部11で受信したパケットの送信元ポート番号を示し、「ディスティネーションIPアドレス」の列は、WANインターフェース部11で受信したパケットの宛先IPアドレスを示し、「プロトコル、ディスティネーションポート番号」の列は、WANインターフェース部11で受信したパケットの宛先ポート番号(ここでは、ポート番号に対応したプロトコル名により示している)を示し、「動作」の列は、WANインターフェース部11で受信

したパケットの送信元情報と宛先情報が、通過条件テーブル(アクセス制御テーブル)48a中のソースIPアドレス及びソースポート番号とディスティネーションIPアドレス及びプロトコル、ディスティネーションポート番号とそれぞれ一致した行に示される動作を、そのパケットに対して行うことを示している。

[0072] なお、「プロトコル、ディスティネーションポート番号」の列で使用されるプロトコル名とポート番号との対応はあらかじめ設定されている。また、「プロトコル、ディスティネーションポート番号」の列には数値、つまりポート番号そのものを設定してもかまわない。

例えば、図30の通過条件の1行目では、ソースIPアドレス及びソースポート番号は「any(任意)」であるから、これらIPアドレス及びポート番号に関係なく、宛先IPアドレスが「111. 111. 111. 2」でかつ宛先ポート番号が「http(Hypertext Transport Protocol、例えばTCP(Transmission Control Protocol)80)」であるパケットは、LAN12に転送される(通過:accept)。

[0073] 図30の通過条件の2行目では、送信元IPアドレスが「123. 123. 123. 1」で、宛先IPアドレスの上位が「111. 111. 111」でかつ宛先ポート番号が「https(Hypertext Transfer Protocol Security、例えばTCP443)」であるパケットは、LAN300に転送され、3行目では、送信元及び宛先の欄はいずれも「any」であり、「動作」の欄は「廃棄」であるから、全てのパケットが廃棄される(廃棄:drop)。

アクセス制御部46中の検索部46aは、このような通過条件テーブル48aを上の行から、受信したパケットの送信元及び送信先情報と一致するか検証し、一致すれば指定された動作を転送制御部46bで行い、そのパケットに対する処理は終了する。この例では、図30の通過条件テーブル48aに対し、上の行に設定された条件がより優先的に処理される条件となっている。

[0074] 図29も参照してアクセス制御部46の動作を具体的に説明する。ファイアウォール装置40のアドレス宛のhttpsの通過条件設定要求パケットを受信すると(ステップS81)、WAN200に接続された送信元の利用者端末220と安全なセッション(SSL(Secure Socket Layer)セッション)の確立をセッション確立・切断部46cで行う(ステップS82)。セッションが正常に確立されれば、セッション確立時に取得した送信元利

用者端末220のIPアドレスを、例えばデータベース部48に記憶する(ステップS83)。また、通信情報生成部46dの要求部46d1により、認証情報要求を利用者端末220へ送信する(ステップS84)。例えばユーザの識別情報とパスワードを入力させるHTMLファイルを暗号化し、要求元の利用者端末220にWANインターフェース部11を介して送信する。この例では要求元の利用者端末220のIPアドレスの他に、その条件設定要求パケット中に含まれる他の条件もデータベース部の通過条件テーブル(アクセス制御テーブル)48aに記憶する。

[0075] 要求元利用者端末220から、暗号化されたユーザの識別情報とパスワードを受信すると(ステップS85)、この暗号化された認証情報を復号化部46eにより復号化を行い(ステップS86)、復号化されたユーザの識別情報とパスワードを認証処理部47に送信して、ユーザの認証を要求する(ステップS87)。

認証処理部47は、ユーザの識別情報とパスワードを受信すると、データベース部48中の認証情報部48bに蓄積してあるユーザの情報から、受信したユーザ識別情報と一致する識別情報を持つユーザを検索する。一致するユーザが見つかれば、認証情報部48bに蓄積してあるそのユーザのパスワードと、受信したパスワードとを比較し、一致していれば、認証正常をアクセス制御部46に送信する。一致するユーザがない場合、またはパスワードが一致しなかった場合は、認証処理部47は認証異常をアクセス制御部46に送信する。

[0076] アクセス制御部46は、認証処理部47から認証正常(合格)を受信すると(ステップS88)、認証正常となったユーザの通過条件設定要求の情報に基づき、パケットの通過を許可する行を通過条件テーブル(アクセス制御テーブル)48aに追加する(ステップS89)。

例えば、認証正常となったIPアドレス「123. 123. 111. 1」の要求元利用者端末220に、IPアドレス「111. 111. 111. 3」のサーバ(例えばLAN300に接続されたWebサーバ310)のftp(File Transfer Protocol)へのアクセスを許可する(通過させる)場合、図31に示すように、図30の通過条件テーブル28aの一番上の行に、要求元利用者端末220及びWebサーバ310のアドレス情報と「動作」が「通過」のアクセス制御ルール(通過条件)を追加する。一般の通過条件としては、送信元アドレスは「any」

でも良いが、この例では要求元利用者端末220のIPアドレスも設定する。

[0077] 次に、アクセス制御部46は、認証が正常であったこと、アクセスが許可されたこと、アクセス可能情報(アクセスが許可されたサービス名(例えば、Webカメラなど)あるいはIPアドレスとポート番号)、通信状況(IPアドレス「123. 123. 111. 1」の利用者端末220と、IPアドレス「111. 111. 111. 3」、ポート番号「ftp」のサーバ310とが通信中であること)などを表示するHTMLファイルを、通知情報生成部46dの許可部46d2及び状況部46d3で生成し、暗号化部46fで暗号化し、要求元利用者端末220に送信する(ステップS90)。

[0078] 利用者端末220では、このファイアウォール装置40から送信されたHTMLファイルを復号化して表示することにより、アクセス可能情報や、アクセス状況を表示することができる。

このように確立した利用者端末220とWebサーバ310とのSSLセッション中において、アクセス制御部46は、利用者端末220からのアクセスを監視部46gで監視し(ステップS91)、利用者端末220からのアクセスの異常を異常検出部46g1で検出すると(ステップS92)、その異常通知を通知情報生成部46dの異常部46d4で生成し、そのSSLセッションを通して利用者端末220へ送信する(ステップS93)。具体的には、例えば以下の通りである。

[0079] (1)利用者端末からのパケットの単位時間当たりのトラヒック(例えば、MB/sなど)は、動画サービス、音声サービスなどのサービスごとにほぼ一定している。そこで、アクセス制御部46は、SSLセッションが確立している端末からのパケットの単位時間当りのトラヒックを監視し、サービスごとにあらかじめ設定されたトラヒック量を超えたトラヒックが発生したときは、そのサービス名や発生したトラヒック量などを表示するHTMLファイルを、暗号化してその利用者端末220に送信する。利用者端末220では、送信されたHTMLファイルを復号化して表示することにより、異常と思われるアクセスの情報が表示され、その利用者端末220の利用者は不正なアクセスがあることを知ることができる。

[0080] (2)利用者端末220から、その利用者端末220に許可されていないサービスに対するアクセス要求があると、その数をサービス毎に計数しておき、その計数の値があらか

じめ設定された値、例えば1を超えたときは、そのサービス名や計数値などを表示するHTMLファイルを暗号化してその利用者端末220に送信する。これを受信した利用者端末220では、送信されたHTMLファイルを復号化して表示することにより、その利用者はその利用者端末220とセッションを確立していないサーバまたは端末に対し、不正なアクセスがあったことを知ることができる。

[0081] (3)同一の利用者端末220からのファイアウォール装置40へのhttpsのアクセス要求パケット(通過条件設定要求に基づくユーザ認証での異常の回数)を計数しておき、その計数の値があらかじめ設定された値を超えたときは、認証異常の回数が異常である旨とその計数値などを表示するHTMLファイルを暗号化してその利用者端末220に送信する。このような異常通知を受信した利用者端末220では、送信されたHTMLファイルを復号化して表示する。この表示によって、正規の利用者になりすました不正なアクセスがあった場合には、正規の利用者は不正なアクセスがあったことを知ることができる。

[0082] 以上のようにしてアクセスを許可され、LAN300内のサーバ310との通信を行った利用者が、通信を終了するときは、ファイアウォール装置40から受信し、その利用者端末220にHTMLファイルで表示された画面から、通信の終了のボタンを選択するか、SSLセッションを切断する。

ファイアウォール装置40のアクセス制御部46は、通信終了のパケットを受信した場合や、SSLセッションの切断を検出した場合には(ステップS94)、図31に示したように書き替えた通過条件テーブル48aを、図30に示した元の状態に戻す(ステップS95)。通信終了パケット受信の場合は、通過条件テーブル48aを元の状態に戻すと共に、そのSSLセッションを切断する。

[0083] ステップS94で通信が終了またはセッションが切断になっていなければ、ステップS81に戻る。ステップS81で通過条件設定要求がなければ、ステップS91に飛びアクセス監視を行う。ステップS88で認証が合格しなければ、ステップS96でセッション確立・切断部46cにより、そのSSLセッションを切断してステップS81に飛ぶ。

なおステップS91, S92及びS93は通信状況監視ステップを構成している。また、図28中において、制御部49は各部を順次動作させることや、データベース部48に

対する読み出し書き込み、消去などを行う。

[0084] 以上述べたように、この実施例では、httpsのセッション内でユーザ(利用者)の認証を行い、認証が正常であれば、そのユーザに対応したアクセス許可(通過条件)をそのhttpsセッションを要求してきたIPアドレスに追加設定しているので、ファイアウォール装置40の外側からファイアウォール装置40のセキュリティポリシー(通過条件)をより安全に変更することができる。しかもセッションが切断されると、その追加設定した通過条件を直ちに削除するため、不正なアクセスを防止できる。

また、この実施例では追加設定の通過条件に認証された通過条件設定要求元の端末のIPアドレス情報が含まれているので、この点からも不正アクセスを防止できる。

[0085] さらに、そのhttpsセッションにアクセスを許可したサービス名や、アクセスを許可したIPアドレスとの通信状況をユーザに表示しているので、これをユーザが確認することにより不正なアクセスを防ぐことができる。

また、ユーザの要求により、またはhttpsセッションの切断により、そのhttpsセッションを利用する通信が終了すれば直ちに変更したアクセス許可(通過条件)の設定状態を元に戻しているので、変更した通過条件設定を利用しての不正アクセスを防ぐことができる。

[0086] [実施例6]

実施例1から5では利用者の端末単位で、アクセス制御ルール(通過条件)を定めたが、ネットワーク単位でのアクセス制御ルールの追加要求(通過条件設定要求)に対しても、この発明を適用できる。

本実施例では、ネットワーク単位でのアクセス制御ルール(通過条件)の追加方法を、実施例5で示した構成に適用した例を示す。例えば、図28中に破線で示す家庭内のホームネットワーク210がWAN200に接続され、このホームネットワーク210に複数の利用者端末220が接続されているとする。この場合、認証時に、ユーザの識別情報とパスワードとともにネットワーク単位での通過条件設定要求が送信され、ユーザのアクセス情報に基づき、ネットワーク単位でのアクセスを許可する設定がされる。つまり、アクセス制御部46は、SSLセッション確立時に取得したIPアドレスのネットワークアドレスに対し、アクセスの許可(「動作」を「通過」にした通過条件)を設定する

。

[0087] 例えば、ネットワーク210に接続された利用者端末(IPアドレスが123. 123. 111. 0／24(上位24ビットが123. 123. 111、下位ビットが0, 1, 2, …, 254のいずれか))に対して、IPアドレス111. 111. 111. 3のサーバ310のftp(File Transfer Protocol)へのアクセスを許可する場合、図30に示した通過条件テーブル48aの一番上の行に、ネットワーク210のネットワークアドレス(IPアドレスの上位24ビットが123. 123. 111であるIPアドレス)をソースIPアドレスとする通過条件を追加する。追加後には、図32のようになる。

[0088] このようにすることにより、SSLセッションが確立中はネットワーク210内の利用者端末220のいずれからのアクセスでも許可することができ、しかもネットワーク210内のブラウザを持たない利用者端末からも許可された宛先に対しアクセスできるようになる。なお、通信状況はそのSSLセッション確立要求、つまり通過条件設定要求を行ったブラウザを持つ利用者端末へ送る。

[0089] [実施例7]

実施例6は、実施例5のファイアウォール装置40に対して、ネットワーク単位でのアクセス制御ルール(通過条件)の追加を行ったが、本実施例では、実施例1の中継装置10に対して、ネットワーク単位でのアクセス制御ルール(通過条件)の追加を行う場合を示す。

例えば、図2中に破線で示す家庭内のホームネットワーク210がWAN200に接続され、このホームネットワーク210に複数の利用者端末220が接続されているとする。この場合、認証時に、ユーザの識別情報とパスワードとともにネットワーク単位での通過条件設定要求が送信され、ユーザのアクセス情報に基づき、ネットワーク単位でのアクセスを許可する設定がされる。つまり、アクセス制御部13は、SSLセッション確立時に取得したIPアドレスのネットワークアドレスに対し、アクセスの許可(「動作」を「通過」にした通過条件)を設定する。

[0090] 例えば、ネットワーク210に接続された利用者端末(IPアドレスが123. 123. 111. 0／24(上位24ビットが123. 123. 111、下位ビットが0, 1, 2, …, 254のいずれか))に対して、IPアドレス111. 111. 111. 3のサーバ310のftp(File Transfer

Protocol)へのアクセスを許可する場合、図3に示したアクセス制御テーブルの一番上の行に、ネットワーク210のネットワークアドレス(IPアドレスの上位24ビットが123. 123. 111であるIPアドレス)をソースIPアドレスとする通過条件を追加する。追加後には、図33のようになる。

[0091] このようなネットワーク単位でのアクセス制御ルールの追加をした上で、ネットワーク210の個々の端末220ごとにアドレス変換ルールを追加する方法もある。

このようにすることにより、SSLセッションが確立中はネットワーク210内の利用者端末220のいずれからのアクセスでも許可することができ、しかもネットワーク210内のブラウザを持たない利用者端末からも許可された宛先に対しアクセスできるようになる。

[0092] [実施例8]

実施例5または6に対する追加の処理として、以下の処理がある。利用者端末220のIPアドレスまたネットワークアドレスに対する通過条件が追加され、利用者端末220とのSSLセッションが確立している時に、その利用者端末220から異なる宛先への接続を要求するパケットを受信することも考えられる。具体的には、ファイアウォール装置40とのSSLセッションが確立している利用者端末の利用者が、例えば現に受けているサービス以外のサービスを受けたい場合などである。このような場合には、すでに確立しているSSLセッションにより、新しい接続要求を許可するか否かをその利用者端末に問い合わせるようにしてもよい。

[0093] 具体的には、利用者端末220は、確立中のSSLセッションを用いて新しい通過条件設定要求を、アクセス制御部46に送信する。アクセス制御部46は、図29中のステップS81の次に破線で示すように、追加設定処理S97を行う。この追加設定処理手順(ステップS97)の例を図34に示す。アクセス制御部46は、受信した通過条件設定要求の要求元IPアドレスが、確立中のSSLセッションの利用者端末220からの追加設定要求であるかを調べる(ステップS97a)。確立中のSSLセッションの利用端末220からの追加設定要求であれば、その利用者端末220に対して、アクセス可能情報やアクセス状況などとともに追加設定要求のパケットを受信した旨と、その追加設定要求の宛先のIPアドレス及びポート番号と、この追加設定要求を許可するか否かを

選択させるボタンを表示するHTMLファイルを通知情報生成部46dで生成し、暗号化してそのSSLセッションを用いて利用者端末220へ送信する(ステップS97b)。

[0094] これを受信した利用者端末220では、その送信されたHTMLファイルを復号化して表示することにより、追加設定要求が受信されたことが利用者端末220の利用者に通知される。したがって、その追加設定要求が利用者の承知しているものであるかをその利用者に確認させることができる。

要求に対する回答が受信されると(ステップS97c)、アクセス制御部46でその回答をチェックする。その利用者端末220からの回答が、「その追加設定を許可する。(追加通過条件設定を認める。)」であれば(ステップS97d)、アクセス制御部46は、その追加設定要求の通過条件を通過条件テーブル48aに追加設定する(ステップS97e)。その後は、追加された通過条件を満すパケットは、既に確立しているSSLセッションにより、LAN内の宛先のサーバに転送される。なお、ステップS97dで利用者端末からの回答が、「接続を拒否する。」であれば、アクセス制御部46は、新たな接続要求(追加設定要求)のパケットを廃棄する(ステップS97f)。

上記の方法では、異なるサービスを提供するサーバへの接続のために、確立済のSSLセッションを利用して、通過条件テーブル48aに新しい通過条件を追加した。別の方法として、以下のように処理することもできる。アクセス制御部46が図34に示したステップS97a, S97b, S97c及びS97dの処理を行い、ステップS97dの回答が許可であれば、そのサービス要求パケットを対応するサーバへ転送する(ステップS97eの括弧書)ようにしてもよい。つまり、確立したSSLセッションを用いて、要求元の利用者端末220からの追加条件設定要求や他宛先へのアクセス要求などに対しては、認証処理を特に行うことなく、既に確立済のSSLセッションを用いて宛先サーバへ転送させてもよい。

[0095] 上記の方法は、新しい接続要求を許可するか否かを、SSLセッションを用いてその利用者端末220の利用者に問い合わせるので、不正なアクセスを防ぐことができる。

なお、この実施例5から7では、利用者端末からの安全なセッションとしてhttpsを用いたが、SSH(Secure Shell)などによる安全なセッションを使っても良い。また、ファイアウォール装置40に、図28に破線で示すようにサーバ310が直接接続されていても

よい。また、通過条件設定要求があれば、その要求元端末と安全なセッションを先ず確立し、その後認証処理を行ったが、先ず認証処理を行ってもよい。つまりステップS81で通過条件設定要求が受信されると図29中に破線で示すように直ちにステップS84に移り、認証処理を行い、その認証に合格すれば、ステップS89でデータベース部48にその通過条件を設定し、かつ要求元端末との間に安全なセッションを確立してもよい。また、認証処理部47をファイアウォール装置40内に設けたが、外部に設けてもよいし、例えばLAN300に接続された認証サーバであってもよい。その場合はデータベース部48から認証情報部48bは省略される。さらに認証処理としてはユーザ識別情報及びパスワードを要求し、これが認証情報部48b内に在るかないかで認証の合格か否かを決定したが、認証サーバを用いることで、より安全度が高い認証方法を利用することも可能となる。

[0096] 実施例1から8に示した中継装置、アドレス変換装置、ファイアウォール装置(アクセス制御装置)をコンピュータにより機能させてもよい。この場合は各処理フローをコンピュータに実行させるプログラムを、コンピュータ内にCD－ROM、磁気ディスク、半導体記憶装置などの記録媒体からインストールし、または通信回線を介してダウンロードして、そのコンピュータにそのプログラムを実行させればよい。

請求の範囲

[1] グローバルネットワークでのアドレスを持たないプライベートネットワークの端末またはサーバが、前記グローバルネットワークを介して通信を行うための中継装置であって、

前記グローバルネットワークとの通信を行うWANインターフェース部と、

前記プライベートネットワークとの通信を行うLANインターフェース部と、

送信元の装置または送信元のネットワークごとに定めたアクセス制御ルールに従って、前記グローバルネットワークから前記プライベートネットワークへのアクセスを制御する手段を有するアクセス制御部と、

送信元の装置ごとに定めたアドレス変換ルールに従って、前記グローバルネットワーク側の端末からの情報を前記プライベートネットワーク側の端末に伝えるためにアドレスの変換を行う手段と、

送信元の装置ごとに定めたアドレス変換ルールに従って、前記プライベートネットワーク側の端末からの情報を前記グローバルネットワーク側の端末に伝えるためにアドレスの変換を行う手段と

を有するアドレス変換部と、

前記アクセス制御ルールと前記アドレス変換ルールとを記録するデータベース部と、

を備える中継装置。

[2] 請求項1記載の中継装置であって、

前記グローバルネットワーク側の端末からのアクセス許可の依頼を受けると、認証処理を行う認証処理部と、

前記認証処理部が認証を行うために用いる利用者情報も記録する前記データベース部と、

前記認証が正常に終了した場合には、送信元の装置または送信元のネットワークごとに定めたアクセス制御ルールを前記データベース部に追加する手段と、

あらかじめ定めた通信終了の判断基準を満足すると、当該追加したアクセス制御ルールを前記データベース部から削除する手段も

有する前記アクセス制御部と、

前記認証が正常に終了した場合には、送信元の装置ごとに定めたアドレス変換ルールを前記データベース部に追加する手段と、

あらかじめ定めた通信終了の判断基準を満足すると、当該追加したアドレス変換ルールを前記データベース部から削除する手段も

有する前記アドレス変換部と、

を備える中継装置。

[3] 請求項1記載の中継装置であって、

グローバルネットワーク側の端末の認証を行う認証処理サーバからの要求があると、送信元の装置または送信元のネットワークごとに定めたアクセス制御ルールを前記データベース部に追加する手段と、

あらかじめ定めた通信終了の判断基準を満足すると、当該追加したアクセス制御ルールを前記データベース部から削除する手段も

有する前記アクセス制御部と、

前記認証サーバからの要求があると、送信元の装置ごとに定めたアドレス変換ルールを前記データベース部に追加する手段と、

あらかじめ定めた通信終了の判断基準を満足すると、当該追加したアドレス変換ルールを前記データベース部から削除する手段も

有する前記アドレス変換部と、

を備える中継装置。

[4] 請求項3記載の中継装置へのアクセスを許可する認証サーバであって、

前記グローバルネットワーク側の端末及び前記中継装置との通信を行うインターフェース部と、

前記グローバルネットワークの端末からの前記中継装置へのアクセス許可の依頼を受けると、認証処理を行う認証処理部と、

前記認証処理部での認証が合格した場合に、前記グローバルネットワークの端末からのパケットのアクセス制御ルールとアドレス変換ルールの追加を、前記中継装置へ要求する手段と、

あらかじめ定めた通信終了の判断基準を満足すると、当該追加したアクセス制御ルールとアドレス変換ルールの削除を、前記中継装置へ要求する手段と
を有する制御部と

前記認証処理部が認証を行うために用いる利用者情報と、追加を要求したアクセス制御ルールとアドレス変換ルールとを関連つける情報とを記録するデータベース部と
を備える認証サーバ。

[5] 請求項1から3のいずれかに記載の中継装置であって、

プライベートネットワーク側の端末からの通信開始要求があると、送信元の装置ごとに定めたアクセス制御ルールを前記データベース部に追加する手段と、
あらかじめ定めた通信終了の判断基準を満足すると、当該追加したアクセス制御ルールを前記データベース部から削除する手段も
有する前記アクセス制御部と、

プライベートネットワーク側の端末からの通信開始要求があると、送信元の装置ごとに定めたアドレス変換ルールを前記データベース部に追加する手段と、
あらかじめ定めた通信終了の判断基準を満足すると、当該追加したアドレス変換ルールを前記データベース部から削除する手段も
有する前記アドレス変換部と、

を備える中継装置。

[6] グローバルネットワークでのアドレスを持たないプライベートネットワークの端末またはサーバが、前記グローバルネットワークを介して通信を行うためのアドレス変換装置であって、

前記グローバルネットワークとの通信を行うWANインターフェース部と、

前記プライベートネットワークとの通信を行うLANインターフェース部と、

送信元の装置ごとに定めたアドレス変換ルールに従って、前記グローバルネットワーク側の端末からの情報を前記プライベートネットワーク側の端末に伝えるためにアドレスの変換を行う手段と、
送信元の装置ごとに定めたアドレス変換ルールに従って、前記プライベートネットワーク側の端末からの情報を前記グローバルネットワーク側の端末に伝えるためにアド

レスの変換を行う手段と

を有するアドレス変換部と、

前記アドレス変換ルールを記録するデータベース部と、

を備えるアドレス変換装置。

[7] 請求項6記載のアドレス変換装置であって、

グローバルネットワーク側の端末またはプライベートネットワーク側の端末からの通信開始要求があると、送信元の装置ごとに定めたアドレス変換ルールを前記データベース部に追加する手段と、

あらかじめ定めた通信終了の判断基準を満足すると、当該追加したアドレス変換ルールを前記データベース部から削除する手段も

有する前記アドレス変換部と、

を備えるアドレス変換装置。

[8] 請求項7記載のアドレス変換装置であって、

グローバルネットワーク側の端末からの通信開始要求があると、認証処理を行う認証処理部と、

前記認証処理部が認証を行うために用いる利用者情報も記録する前記データベース部と、

グローバルネットワーク側の端末からの通信開始要求に対しては、前記認証が正常に終了した場合に限り、前記アドレス変換ルールを前記データベース部に追加する前記アドレス変換部と、

を備えるアドレス変換装置。

[9] 請求項7記載のアドレス変換装置であって、

グローバルネットワーク側の端末からの通信開始要求に対しては、認証処理を行う認証処理サーバからの要求がある場合に限り、前記アドレス変換ルールを前記データベース部に追加する前記アドレス変換部

を備えるアドレス変換装置。

[10] 請求項9記載のアドレス変換装置へのアクセスを許可する認証サーバであって、

前記グローバルネットワーク側の端末及び前記中継装置との通信を行うインターフ

ェース部と、

前記グローバルネットワークの端末からの前記中継装置へのアクセス許可の依頼を受けると、認証処理を行う認証処理部と、

前記認証処理部での認証が合格した場合に、前記グローバルネットワークの端末からのパケットのアドレス変換ルールの追加を、前記アドレス変換装置へ要求する手段と、

あらかじめ定めた通信終了の判断基準を満足すると、当該追加したアドレス変換ルールの削除を、前記アドレス変換装置へ要求する手段と

を有する制御部と

前記認証処理部が認証を行うために用いる利用者情報を記録するデータベース部と

を備える認証サーバ。

[11] ファイアウォール装置外のグローバルネットワークからのパケットがデータベース部に設定されている通過条件を満すと、そのパケットをファイアウォール装置内のプライベートネットワークに通過させるファイアウォール装置であって、

前記グローバルネットワークとの通信を行うWANインターフェース部と、

前記プライベートネットワークとの通信を行うLANインターフェース部と、

送信元の装置または送信元のネットワークごとに定めたアクセス制御ルールに従って、前記グローバルネットワークから前記プライベートネットワークへのアクセスを制御する手段を有するアクセス制御部と、

前記グローバルネットワークからのアクセス許可の依頼を受けると、認証処理を行う認証処理部と、

前記アクセス制御ルールと前記認証処理部が認証を行うために用いる利用者情報とを記録するデータベース部と、

を備えるファイアウォール装置。

[12] 請求項11記載のファイアウォール装置であって、

前記グローバルネットワークの装置からのアクセス許可の依頼に対応するアクセス制御ルールが、前記データベース部に記録されていない場合に、

前記認証処理部での認証が正常に終了すると、送信元の装置または送信元のネットワークごとに定めたアクセス制御ルールを前記データベース部に追加する手段と、あらかじめ定めた通信終了の判断基準を満足すると、当該追加したアクセス制御ルールを前記データベース部から削除する手段も

有する前記アクセス制御部

を備えるファイアウォール装置。

[13] 請求項12記載のファイアウォール装置であって、

安全なセッション確立中に、当該セッションを使用しているグローバルネットワークの装置からの新たなアクセス許可の依頼があった場合に、

前記安全なセッションを用いて、前記グローバルネットワークの装置に対して前記依頼の内容を確認する通知を送る手段と、

前記グローバルネットワークの装置からの拒否の回答を得た場合に、前記アクセス制御ルールに関わりなく、新たなアクセスを拒否する手段も

有する前記アクセス制御部

を備えるファイアウォール装置。

[14] 請求項11から13のいずれかに記載のファイアウォール装置であって、

通信状況の監視を行う手段と、

あらかじめ定めた通信異常の基準を満足する場合に、通信の異常を前記グローバルネットワークの装置に通知する手段

も有する前記アクセス制御部

を備えるファイアウォール装置。

[15] グローバルネットワークでのアドレスを持たないプライベートネットワークの端末が、前記グローバルネットワークを介して通信を行うためのアドレス変換方法であって、

あらかじめ送信元の装置ごとに定めたアドレス変換ルールをデータベース部に記録しておき、

前記グローバルネットワーク側からのパケットをWANインターフェース部が受信すると、

前記アドレス変換ルールに従って、アドレス変換部で宛先アドレスを変換し、

LANインターフェース部が、当該アドレス変換されたパケットを前記プライベートネットワーク側に伝え、

前記プライベートネットワーク側からのパケットをLANインターフェース部が受信すると、

前記アドレス変換ルールに従って、アドレス変換部で送信元アドレスを変換し、

WANインターフェース部が、当該アドレス変換されたパケットを前記グローバルネットワーク側に伝える

ことを特徴とするアドレス変換方法。

[16] グローバルネットワークでのアドレスを持たないプライベートネットワークの端末が、前記グローバルネットワークを介して通信を行うためのアドレス変換方法であって、

あらかじめ送信元の装置ごとに定めたアドレス変換ルールをデータベース部に記録しておき、

前記グローバルネットワーク側からのパケットをWANインターフェース部が受信した場合に、

認証処理部で認証処理を行い、認証が合格すると、

前記アドレス変換部で前記パケットの送信元情報と宛先情報に一致するアドレス変換ルールがデータベース部に記録されていることを調べ、

一致するアドレス変換ルールが存在する場合は、当該アドレス変換ルールに従って前記パケットのアドレスを変換し、

一致するアドレス変換ルールが存在しない場合は、アドレス変換ルールを前記データベース部に追加して、当該追加したアドレス変換ルールに従って前記パケットのアドレスを変換し、

LANインターフェース部が、当該アドレス変換されたパケットを前記プライベートネットワーク側に伝え、

前記プライベートネットワーク側からのパケットをLANインターフェース部が受信した場合に、

前記アドレス変換部で前記パケットの送信元情報と宛先情報に一致するアドレス変換ルールがデータベース部に記録されていることを調べ、

一致するアドレス変換ルールが存在する場合は、当該アドレス変換ルールに従って前記パケットのアドレスを変換し、

一致するアドレス変換ルールが存在しない場合は、アドレス変換ルールを前記データベース部に追加して、当該追加したアドレス変換ルールに従って前記パケットのアドレスを変換し、

WANインターフェース部が、当該アドレス変換されたパケットを前記グローバルネットワーク側に伝え

あらかじめ定めた通信終了の判断基準を満足すると、

前記アドレス変換部で追加したアドレス変換ルールがある場合には、当該アドレス変換ルールを前記データベース部から削除する

ことを特徴とするアドレス変換方法。

[17] 請求項16記載のアドレス変換方法であって、

認証処理部で認証処理を行う代わりに、前記グローバルネットワーク側の端末の認証を行う認証サーバからの要求があると、認証が合格したと判断する

ことを特徴とするアドレス変換方法。

[18] ファイアウォール外のグローバルネットワークからのパケットがデータベース部に設定されているアクセス制御ルールを満すと、そのパケットをファイアウォール内のプライベートネットワークに通過させるアクセス制御方法であって、

あらかじめ送信元の装置または送信元のネットワークごとに定めたアクセス制御ルールをデータベース部に記録しておき、

前記グローバルネットワーク側からの接続要求をWANインターフェース部が受信すると、

アクセス制御部で、接続要求と一致するアクセス制御ルールが前記データベース部に記録されていることを調べ、

アクセス制御ルールが存在する場合には、通信を許可する

ことを特徴とするアクセス制御方法。

[19] ファイアウォール外のグローバルネットワークからのパケットがデータベース部に設定されているアクセス制御ルールを満すと、そのパケットをファイアウォール内のプラ

イベートネットワークに通過させるアクセス制御方法であって、

あらかじめ送信元の装置または送信元のネットワークごとに定めたアクセス制御ルールをデータベース部に記録しておき、

前記グローバルネットワーク側からの接続要求をWANインターフェース部が受信した場合に、

認証処理部で認証処理を行い、認証が合格すると、

アクセス制御部で、接続要求と一致するアクセス制御ルールが前記データベース部に記録されていることを調べ、

一致するアクセス制御ルールが存在する場合は、通信を許可し、

一致するアクセス制御ルールが存在しない場合は、送信元の装置または送信元のネットワークごとに定めたアクセス制御ルールを前記データベース部に追加して、通信を許可し、

前記プライベートネットワーク側からのパケットをLANインターフェース部が受信した場合に、

アクセス制御部で、接続要求と一致するアクセス制御ルールが前記データベース部に記録されていることを調べ、

一致するアクセス制御ルールが存在する場合は、通信を許可し、

一致するアクセス制御ルールが存在しない場合は、送信元の装置ごとに定めたアクセス制御ルールを前記データベース部に追加して、通信を許可し、

あらかじめ定めた通信終了の判断基準を満足すると、

前記アクセス制御部で追加したアクセス制御ルールがある場合には、当該アクセス制御ルールを前記データベース部から削除する

ことを特徴とするアクセス制御方法。

[20] 請求項19記載のアクセス制御方法であって、

認証処理部で認証処理を行う代わりに、前記グローバルネットワーク側の端末の認証を行う認証サーバからの要求があると、認証が合格したと判断する

ことを特徴とするアクセス制御方法。

[21] 請求項18から20のいずれかに記載のアクセス制御方法であって、

安全なセッション確立中は、その通信状況を監視し、

あらかじめ定めた基準に該当する場合には、異常が生じたことを、当該安全なセッションを確立しているグローバルネットワークの装置に通知する

ことを特徴とするアクセス制御方法。

[22] 請求項18から20のいずれかに記載のアクセス制御方法であって、

安全なセッション確立中に、当該安全なセッションを確立しているグローバルネットワークの装置からの新たな接続要求を、WANインターフェース部が受信した場合に、

当該接続要求の内容を、当該安全なセッションを確立しているグローバルネットワークの装置に通知し、

当該装置から、拒否の回答があった場合には、データベース部に記録されているアクセス制御ルールに関わらず、接続を拒否する

ことを特徴とするアクセス制御方法。

補正書の請求の範囲

[2005年9月29日 (29.09.05) 国際事務局受理：出願当初の請求の範囲 10 は補正された；新しい請求の範囲 15-20 が加えられた；出願当初の請求の範囲 15-22 は請求の範囲 21-28 に番号が付け替えられた ；他の請求の範囲は変更なし。]

レスの変換を行う手段と

を有するアドレス変換部と、

前記アドレス変換ルールを記録するデータベース部と、

を備えるアドレス変換装置。

[7] 請求項6記載のアドレス変換装置であって、

グローバルネットワーク側の端末またはプライベートネットワーク側の端末からの通信開始要求があると、送信元の装置ごとに定めたアドレス変換ルールを前記データベース部に追加する手段と、

あらかじめ定めた通信終了の判断基準を満足すると、当該追加したアドレス変換ルールを前記データベース部から削除する手段も

有する前記アドレス変換部と、

を備えるアドレス変換装置。

[8] 請求項7記載のアドレス変換装置であって、

グローバルネットワーク側の端末からの通信開始要求があると、認証処理を行う認証処理部と、

前記認証処理部が認証を行うために用いる利用者情報も記録する前記データベース部と、

グローバルネットワーク側の端末からの通信開始要求に対しては、前記認証が正常に終了した場合に限り、前記アドレス変換ルールを前記データベース部に追加する前記アドレス変換部と、

を備えるアドレス変換装置。

[9] 請求項7記載のアドレス変換装置であって、

グローバルネットワーク側の端末からの通信開始要求に対しては、認証処理を行う認証処理サーバからの要求がある場合に限り、前記アドレス変換ルールを前記データベース部に追加する前記アドレス変換部

を備えるアドレス変換装置。

[10] (補正後)請求項9記載のアドレス変換装置へのアクセスを許可する認証サーバであって、

前記グローバルネットワーク側の端末及び前記アドレス変換装置との通信を行うインターフェース部と、

前記グローバルネットワークの端末からの前記アドレス変換装置へのアクセス許可の依頼を受けると、認証処理を行う認証処理部と、

前記認証処理部での認証が合格した場合に、前記グローバルネットワークの端末からのパケットのアドレス変換ルールの追加を、前記アドレス変換装置へ要求する手段と、

あらかじめ定めた通信終了の判断基準を満足すると、当該追加したアドレス変換ルールの削除を、前記アドレス変換装置へ要求する手段と

を有する制御部と

前記認証処理部が認証を行うために用いる利用者情報を記録するデータベース部と

を備える認証サーバ。

[11] ファイアウォール装置外のグローバルネットワークからのパケットがデータベース部に設定されている通過条件を満すと、そのパケットをファイアウォール装置内のプライベートネットワークに通過させるファイアウォール装置であって、

前記グローバルネットワークとの通信を行うWANインターフェース部と、

前記プライベートネットワークとの通信を行うLANインターフェース部と、

送信元の装置または送信元のネットワークごとに定めたアクセス制御ルールに従って、前記グローバルネットワークから前記プライベートネットワークへのアクセスを制御する手段を有するアクセス制御部と、

前記グローバルネットワークからのアクセス許可の依頼を受けると、認証処理を行う認証処理部と、

前記アクセス制御ルールと前記認証処理部が認証を行うために用いる利用者情報とを記録するデータベース部と、

を備えるファイアウォール装置。

[12] 請求項11記載のファイアウォール装置であって、

前記グローバルネットワークの装置からのアクセス許可の依頼に対応するアクセス

制御ルールが、前記データベース部に記録されていない場合に、

前記認証処理部での認証が正常に終了すると、送信元の装置または送信元のネットワークごとに定めたアクセス制御ルールを前記データベース部に追加する手段と、

あらかじめ定めた通信終了の判断基準を満足すると、当該追加したアクセス制御ルールを前記データベース部から削除する手段も

有する前記アクセス制御部

を備えるファイアウォール装置。

[13] 請求項12記載のファイアウォール装置であって、

安全なセッション確立中に、当該セッションを使用しているグローバルネットワークの装置からの新たなアクセス許可の依頼があった場合に、

前記安全なセッションを用いて、前記グローバルネットワークの装置に対して前記依頼の内容を確認する通知を送る手段と、

前記グローバルネットワークの装置からの拒否の回答を得た場合に、前記アクセス制御ルールに関わりなく、新たなアクセスを拒否する手段も

有する前記アクセス制御部

を備えるファイアウォール装置。

[14] 請求項11から13のいずれかに記載のファイアウォール装置であって、

通信状況の監視を行う手段と、

あらかじめ定めた通信異常の基準を満足する場合に、通信の異常を前記グローバルネットワークの装置に通知する手段

も有する前記アクセス制御部

を備えるファイアウォール装置。

[15] (補正後)請求項1記載の中継装置であって、

前記アクセス制御ルールおよび前記アドレス変換ルールが、送信元の装置のIPアドレスまたは送信元のネットワークのIPアドレスを用いた条件を含む

ことを特徴とする中継装置。

[16] (補正後)請求項15記載の中継装置であって、

前記グローバルネットワーク側の端末からのアクセス許可の依頼を受けると、認証処

理を行う認証処理部と、

前記認証処理部が認証を行うために用いる利用者情報も記録する前記データベース部と、

前記認証が正常に終了した場合には、送信元の装置または送信元のネットワークごとに定めたアクセス制御ルールを前記データベース部に追加する手段と、

あらかじめ定めた通信終了の判断基準を満足すると、当該追加したアクセス制御ルールを前記データベース部から削除する手段も

有する前記アクセス制御部と、

前記認証が正常に終了した場合には、送信元の装置ごとに定めたアドレス変換ルールを前記データベース部に追加する手段と、

あらかじめ定めた通信終了の判断基準を満足すると、当該追加したアドレス変換ルールを前記データベース部から削除する手段も

有する前記アドレス変換部と、

を備える中継装置。

[17] (補正後)請求項6記載のアドレス変換装置であって、

前記アドレス変換ルールが、送信元の装置のIPアドレスまたは送信元のネットワークのIPアドレスを用いた条件を含む

ことを特徴とするアドレス変換装置。

[18] (補正後)請求項17記載のアドレス変換装置であって、

グローバルネットワーク側の端末またはプライベートネットワーク側の端末からの通信開始要求があると、送信元の装置ごとに定めたアドレス変換ルールを前記データベース部に追加する手段と、

あらかじめ定めた通信終了の判断基準を満足すると、当該追加したアドレス変換ルールを前記データベース部から削除する手段も

有する前記アドレス変換部と、

を備えるアドレス変換装置。

[19] (補正後)請求項11記載のファイアウォール装置であって、

前記アクセス制御ルールが、送信元の装置のIPアドレスまたは送信元のネットワー

クのIPアドレスを用いた条件を含む

ことを特徴とするファイアウォール装置。

[20] (補正後)請求項19記載のファイアウォール装置であって、

前記グローバルネットワークの装置からのアクセス許可の依頼に対応するアクセス制御ルールが、前記データベース部に記録されていない場合に、

前記認証処理部での認証が正常に終了すると、送信元の装置または送信元のネットワークごとに定めたアクセス制御ルールを前記データベース部に追加する手段と、あらかじめ定めた通信終了の判断基準を満足すると、当該追加したアクセス制御ルールを前記データベース部から削除する手段も

有する前記アクセス制御部

を備えるファイアウォール装置。

[21] (補正後)グローバルネットワークでのアドレスを持たないプライベートネットワークの端末が、前記グローバルネットワークを介して通信を行うためのアドレス変換方法であって、

あらかじめ送信元の装置ごとに定めたアドレス変換ルールをデータベース部に記録しておき、

前記グローバルネットワーク側からのパケットをWANインターフェース部が受信すると、

前記アドレス変換ルールに従って、アドレス変換部で宛先アドレスを変換し、

LANインターフェース部が、当該アドレス変換されたパケットを前記プライベートネットワーク側に伝え、

前記プライベートネットワーク側からのパケットをLANインターフェース部が受信すると、

前記アドレス変換ルールに従って、アドレス変換部で送信元アドレスを変換し、

WANインターフェース部が、当該アドレス変換されたパケットを前記グローバルネットワーク側に伝える

ことを特徴とするアドレス変換方法。

[22] (補正後)グローバルネットワークでのアドレスを持たないプライベートネットワークの

端末が、前記グローバルネットワークを介して通信を行うためのアドレス変換方法であって、

あらかじめ送信元の装置ごとに定めたアドレス変換ルールをデータベース部に記録しておき、

前記グローバルネットワーク側からのパケットをWANインターフェース部が受信した場合に、

認証処理部で認証処理を行い、認証が合格すると、

前記アドレス変換部で前記パケットの送信元情報と宛先情報に一致するアドレス変換ルールがデータベース部に記録されていることを調べ、

一致するアドレス変換ルールが存在する場合は、当該アドレス変換ルールに従って前記パケットのアドレスを変換し、

一致するアドレス変換ルールが存在しない場合は、アドレス変換ルールを前記データベース部に追加して、当該追加したアドレス変換ルールに従って前記パケットのアドレスを変換し、

LANインターフェース部が、当該アドレス変換されたパケットを前記プライベートネットワーク側に伝え、

前記プライベートネットワーク側からのパケットをLANインターフェース部が受信した場合に、

前記アドレス変換部で前記パケットの送信元情報と宛先情報に一致するアドレス変換ルールがデータベース部に記録されていることを調べ、

一致するアドレス変換ルールが存在する場合は、当該アドレス変換ルールに従って前記パケットのアドレスを変換し、

一致するアドレス変換ルールが存在しない場合は、アドレス変換ルールを前記データベース部に追加して、当該追加したアドレス変換ルールに従って前記パケットのアドレスを変換し、

WANインターフェース部が、当該アドレス変換されたパケットを前記グローバルネットワーク側に伝え

あらかじめ定めた通信終了の判断基準を満足すると、

前記アドレス変換部で追加したアドレス変換ルールがある場合には、当該アドレス変換ルールを前記データベース部から削除する

ことを特徴とするアドレス変換方法。

[23] (追加)請求項22記載のアドレス変換方法であって、

認証処理部で認証処理を行う代わりに、前記グローバルネットワーク側の端末の認証を行う認証サーバからの要求があると、認証が合格したと判断する

ことを特徴とするアドレス変換方法。

[24] (追加)ファイアウォール外のグローバルネットワークからのパケットがデータベース部に設定されているアクセス制御ルールを満すと、そのパケットをファイアウォール内のプライベートネットワークに通過させるアクセス制御方法であって、

あらかじめ送信元の装置または送信元のネットワークごとに定めたアクセス制御ルールをデータベース部に記録しておき、

前記グローバルネットワーク側からの接続要求をWANインターフェース部が受信すると、

アクセス制御部で、接続要求と一致するアクセス制御ルールが前記データベース部に記録されていることを調べ、

アクセス制御ルールが存在する場合には、通信を許可する

ことを特徴とするアクセス制御方法。

[25] (追加)ファイアウォール外のグローバルネットワークからのパケットがデータベース部に設定されているアクセス制御ルールを満すと、そのパケットをファイアウォール内のプライベートネットワークに通過させるアクセス制御方法であって、

あらかじめ送信元の装置または送信元のネットワークごとに定めたアクセス制御ルールをデータベース部に記録しておき、

前記グローバルネットワーク側からの接続要求をWANインターフェース部が受信した場合に、

認証処理部で認証処理を行い、認証が合格すると、

アクセス制御部で、接続要求と一致するアクセス制御ルールが前記データベース部に記録されていることを調べ、

一致するアクセス制御ルールが存在する場合は、通信を許可し、

一致するアクセス制御ルールが存在しない場合は、送信元の装置または送信元のネットワークごとに定めたアクセス制御ルールを前記データベース部に追加して、通信を許可し、

前記プライベートネットワーク側からのパケットをLANインターフェース部が受信した場合に、

アクセス制御部で、接続要求と一致するアクセス制御ルールが前記データベース部に記録されていることを調べ、

一致するアクセス制御ルールが存在する場合は、通信を許可し、

一致するアクセス制御ルールが存在しない場合は、送信元の装置ごとに定めたアクセス制御ルールを前記データベース部に追加して、通信を許可し、

あらかじめ定めた通信終了の判断基準を満足すると、

前記アクセス制御部で追加したアクセス制御ルールがある場合には、当該アクセス制御ルールを前記データベース部から削除する

ことを特徴とするアクセス制御方法。

[26] (追加)請求項25記載のアクセス制御方法であって、

認証処理部で認証処理を行う代わりに、前記グローバルネットワーク側の端末の認証を行う認証サーバからの要求があると、認証が合格したと判断する

ことを特徴とするアクセス制御方法。

[27] (追加)請求項24から26のいずれかに記載のアクセス制御方法であって、

安全なセッション確立中は、その通信状況を監視し、

あらかじめ定めた基準に該当する場合には、異常が生じたことを、当該安全なセッションを確立しているグローバルネットワークの装置に通知する

ことを特徴とするアクセス制御方法。

[28] (追加)請求項24から26のいずれかに記載のアクセス制御方法であって、

安全なセッション確立中に、当該安全なセッションを確立しているグローバルネットワークの装置からの新たな接続要求を、WANインターフェース部が受信した場合に

、

当該接続要求の内容を、当該安全なセッションを確立しているグローバルネットワークの装置に通知し、

当該装置から、拒否の回答があった場合には、データベース部に記録されているアクセス制御ルールに関わらず、接続を拒否する

ことを特徴とするアクセス制御方法。

条約第１９条（１）に基づく説明書

請求の範囲第１０項の２行目及び４行目の語句「中継」をそれぞれ「アドレス変換」に補正した。

請求の範囲第１４項の後に新たに請求項６個を挿入し、各請求項の番号を１５、１６、１７、１８、１９及び２０とした。

請求の範囲第１５項から第２２項の請求項の番号を２１から２８と付け直した。

[図1]

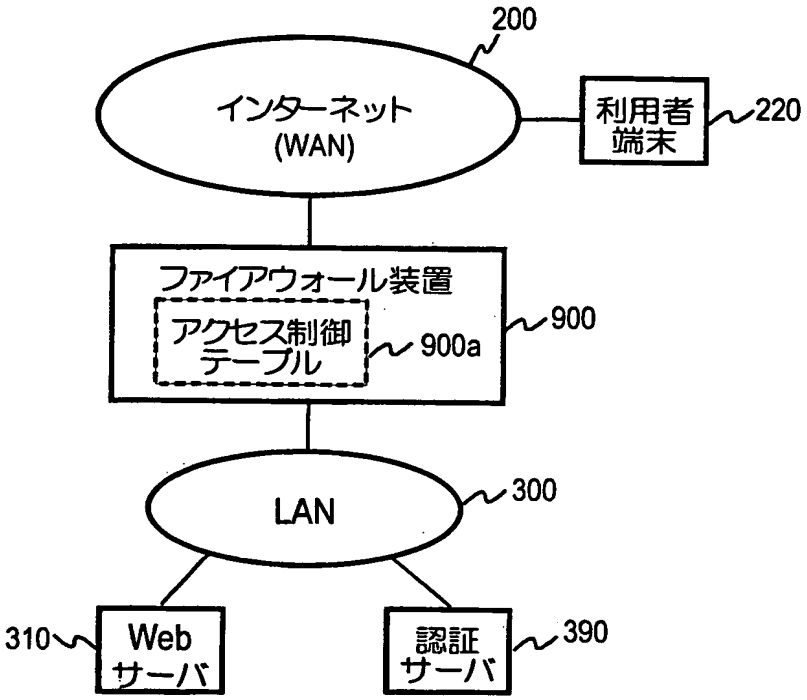

200
インターネット
(WAN)
利用者
端末
220
ファイアウォール装置
アクセス制御
テーブル
900a
900
LAN
300
310
Web
サーバ
認証
サーバ
390

図1

[図2]

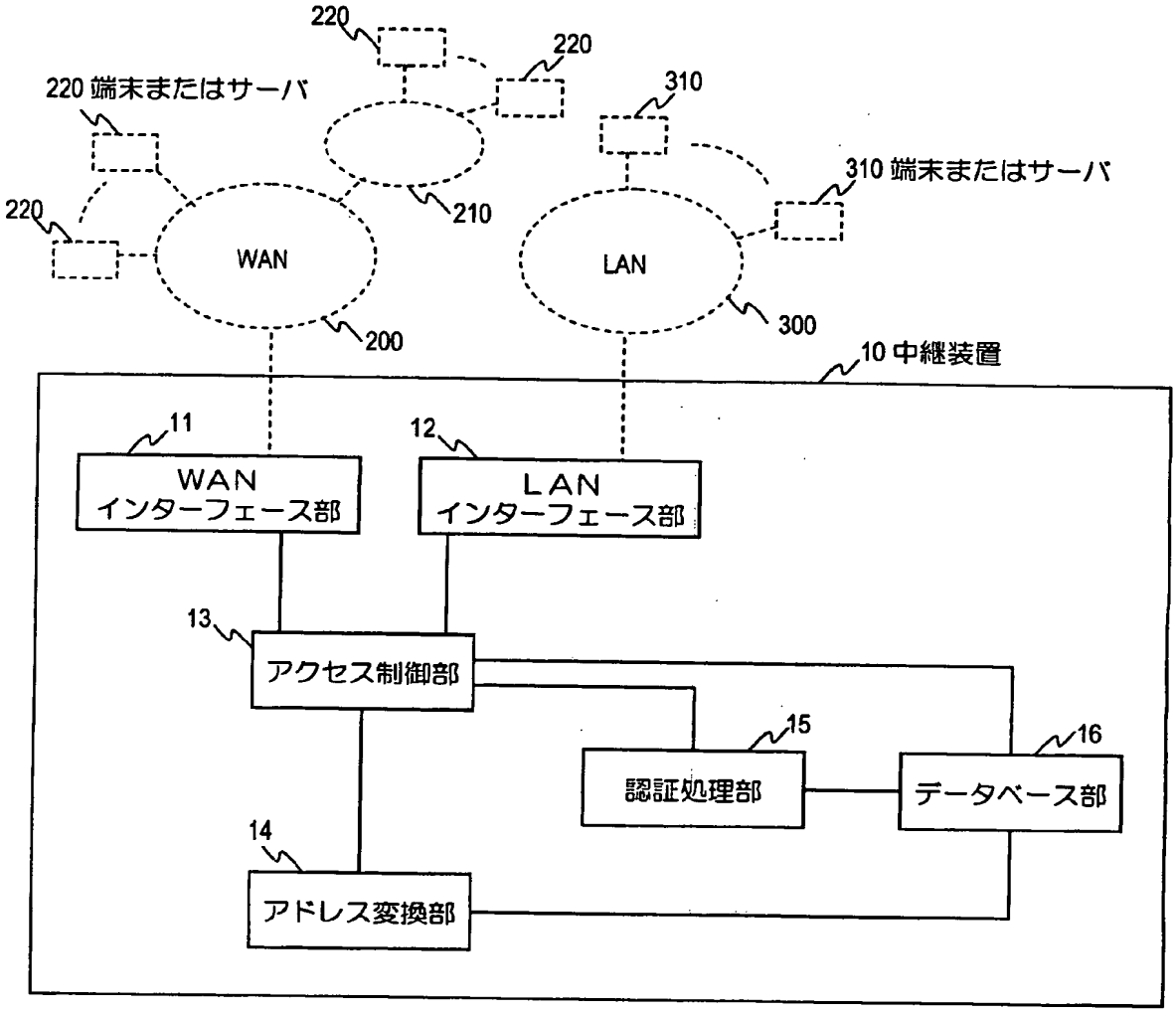

220
220
220 端末またはサーバ
310
310 端末またはサーバ
220
210
WAN
LAN
200
300
10 中継装置
11
12
WAN
インターフェース部
LAN
インターフェース部
13
アクセス制御部
15
16
認証処理部
データベース部
14
アドレス変換部

図2

[図3]

ソース IPアドレス	プロトコル、ソースポート番号	ディスティネーション IPアドレス	プロトコル、ディスティネーションポート番号	動作
any	any	111.111.111.2	http	通過
123.123.123.1	any	111.111.111.2	ssh	通過
any	any	any	any	廃棄

図3

[図4]

ソース IPアドレス	ディスティネーション IPアドレス	プロトコル、ディスティネーションポート番号	内部IPアドレス	プロトコルおよびポート番号
any	111.111.111.2	TCP 80	192.168.100.5	TCP 80
123.123.123.1	111.111.111.2	TCP 22	192.168.100.5	TCP 22

図4

[図5]

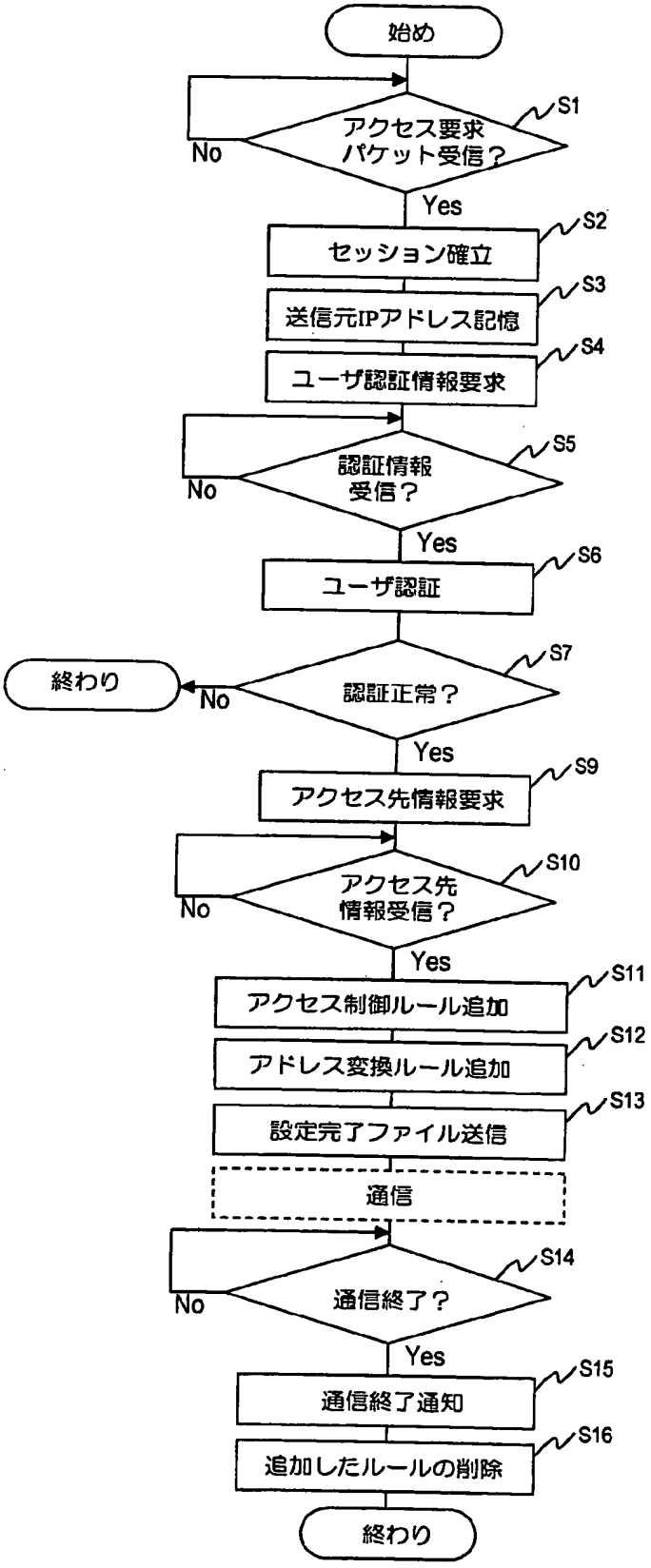

始め
S1
アクセス要求
パケット受信？
No
Yes
S2
セッション確立
S3
送信元IPアドレス記憶
S4
ユーザ認証情報要求
S5
認証情報
受信？
No
Yes
S6
ユーザ認証
S7
終わり
No
認証正常？
Yes
S9
アクセス先情報要求
S10
アクセス先
情報受信？
No
Yes
S11
アクセス制御ルール追加
S12
アドレス変換ルール追加
S13
設定完了ファイル送信
通信
S14
No
通信終了？
Yes
S15
通信終了通知
S16
追加したルールの削除
終わり

図5

[図6]

ソースＩＰアドレス	プロトコル、ソースポート番号	ディスティネーションＩＰアドレス	プロトコル、ディスティネーションポート番号	動作
111.222.234.123	any	111.111.111.2	ssl	通過
any	any	111.111.111.2	http	通過
123.123.123.1	any	111.111.111.2	ssl	通過
any	any	any	any	廃棄

図6

[図7]

ソースＩＰアドレス	ディスティネーションＩＰアドレス	プロトコル、ディスティネーションポート番号	内部ＩＰアドレス	プロトコルおよびポート番号
111.222.234.123	111.111.111.2	TCP 22	192.168.100.4	TCP 22
any	111.111.111.2	TCP 80	192.168.100.5	TCP 80
123.123.123.1	111.111.111.2	TCP 22	192.168.100.5	TCP 22

図7

[図8]

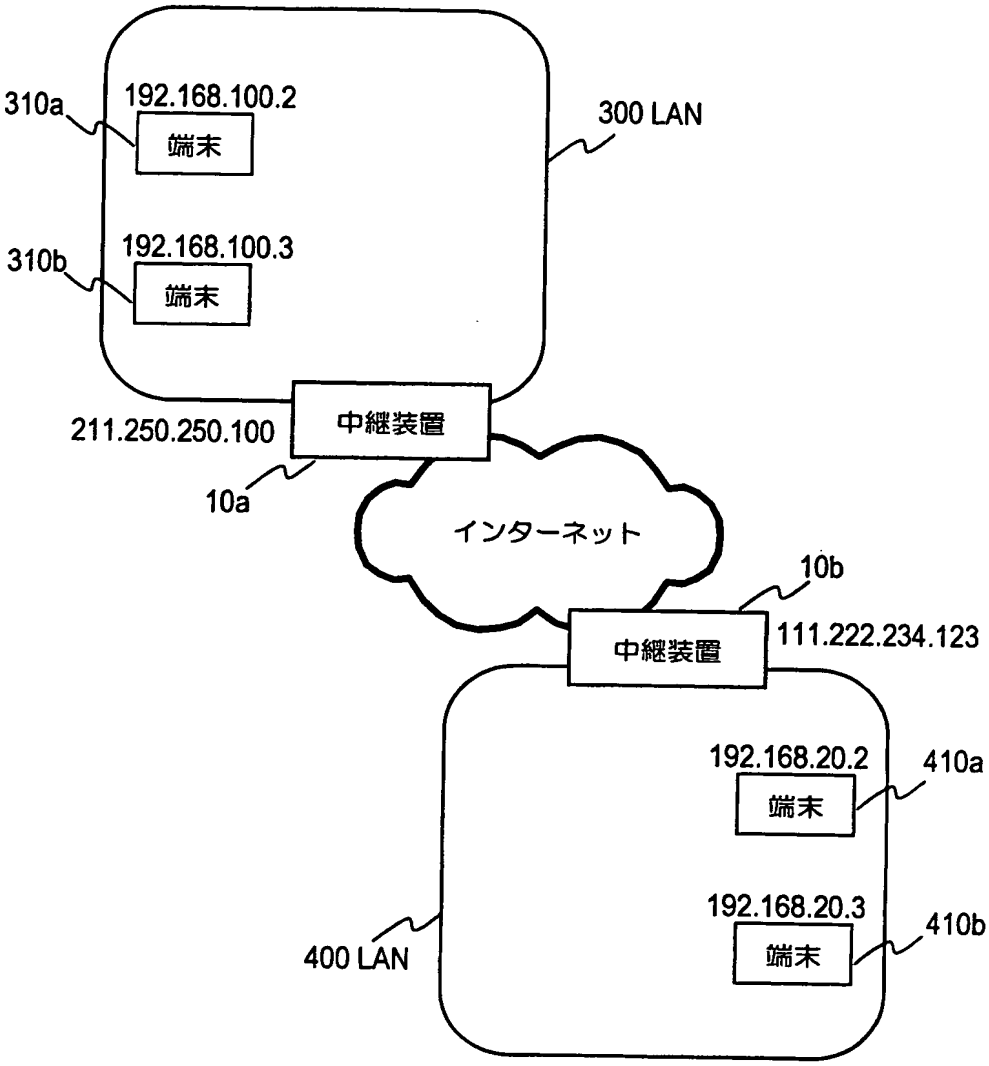

310a
192.168.100.2
端末
300 LAN
310b
192.168.100.3
端末
211.250.250.100
中継装置
10a
インターネット
10b
中継装置
111.222.234.123
192.168.20.2
410a
端末
192.168.20.3
410b
端末
400 LAN

図8

[図9]

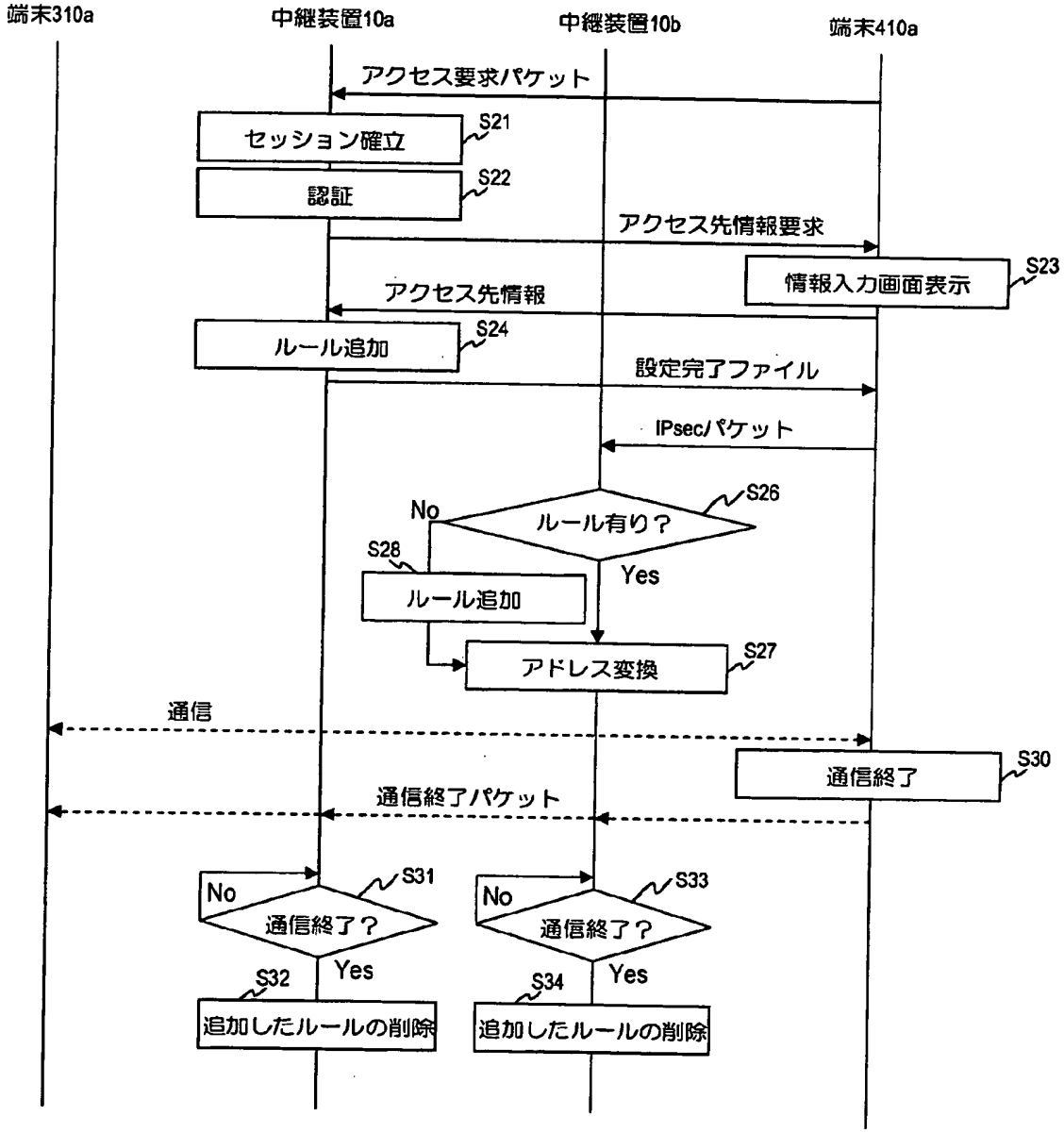

端末310a
中継装置10a
中継装置10b
端末410a
アクセス要求パケット
セッション確立
S21
認証
S22
アクセス先情報要求
情報入力画面表示
S23
アクセス先情報
ルール追加
S24
設定完了ファイル
IPsecパケット
No
ルール有り？
S26
Yes
S28
ルール追加
アドレス変換
S27
通信
通信終了
S30
通信終了パケット
No
通信終了？
S31
Yes
S32
追加したルールの削除
No
通信終了？
S33
Yes
S34
追加したルールの削除

図9

[図10]

ソースＩＰアドレス	プロトコル、ソースポート番号	ディスティネーションＩＰアドレス	プロトコル、ディスティネーションポート番号	動作
111.222.234.123	IPsec	211.250.250.100	IPsec	通過

図１０

[図11]

ソースＩＰアドレス	ディスティネーションＩＰアドレス	プロトコル、ディスティネーションポート番号	内部ＩＰアドレス	プロトコルおよびポート番号
111.222.234.123	211.250.250.100	IPsec	192.168.100.2	IPsec

図１１

[図12]

ソースＩＰアドレス	ディスティネーションＩＰアドレス	プロトコル、ディスティネーションポート番号	内部ＩＰアドレス	プロトコルおよびポート番号
211.250.250.100	111.222.234.123	IPsec	192.168.20.2	IPsec

図１２

[図13]

ソースＩＰアドレス	プロトコル、ソースポート番号	ディスティネーションＩＰアドレス	プロトコル、ディスティネーションポート番号	動作
211.250.250.100	IPsec	111.222.234.123	IPsec	通過

図１３

[図14]

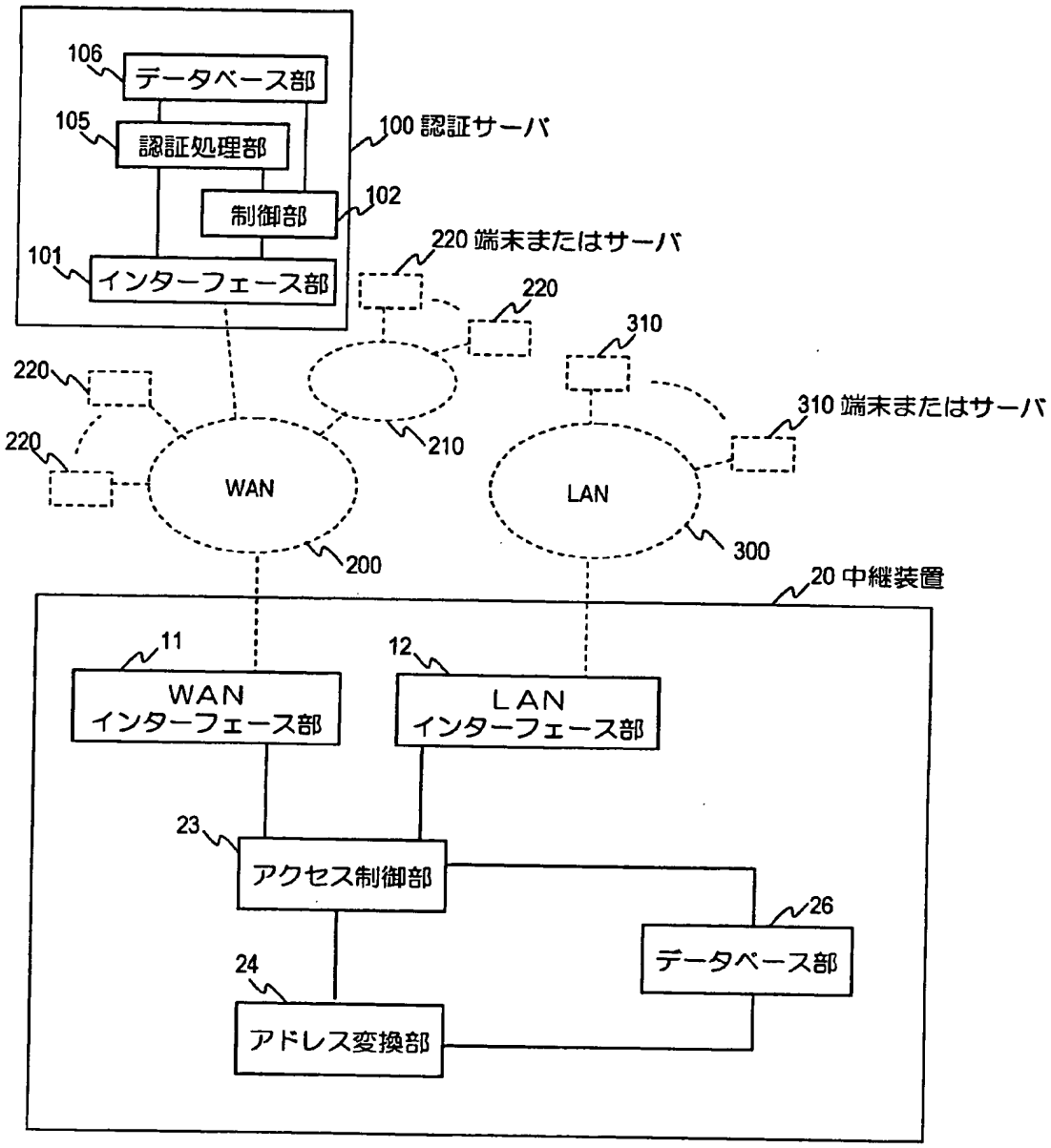

106
データベース部
105
認証処理部
100 認証サーバ
制御部
102
101
インターフェース部
220 端末またはサーバ
220
310
220
310 端末またはサーバ
220
210
WAN
LAN
200
300
20 中継装置
11
12
WAN
インターフェース部
LAN
インターフェース部
23
アクセス制御部
26
データベース部
24
アドレス変換部

図１４

[図15]

ソースＩＰアドレス	ソースポート番号	ディスティネーション ＩＰアドレス	プロトコル、 ディスティネーション ポート番号	動作
any	any	123.123.123.123	https	通過
211.250.250.100	any	123.123.123.123	ssh	通過
any	any	any	any	廃棄

図１５

[図16]

ソースＩＰアドレス	ディスティネーション ＩＰアドレス	プロトコル、 ディスティネーション ポート番号	内部ＩＰアドレス	プロトコルおよび ポート番号
any	123.123.123.123	TCP 443	192.168.100.5	TCP 443
211.250.250.100	123.123.123.123	TCP 22	192.168.100.5	TCP 22

図１６

[図17]

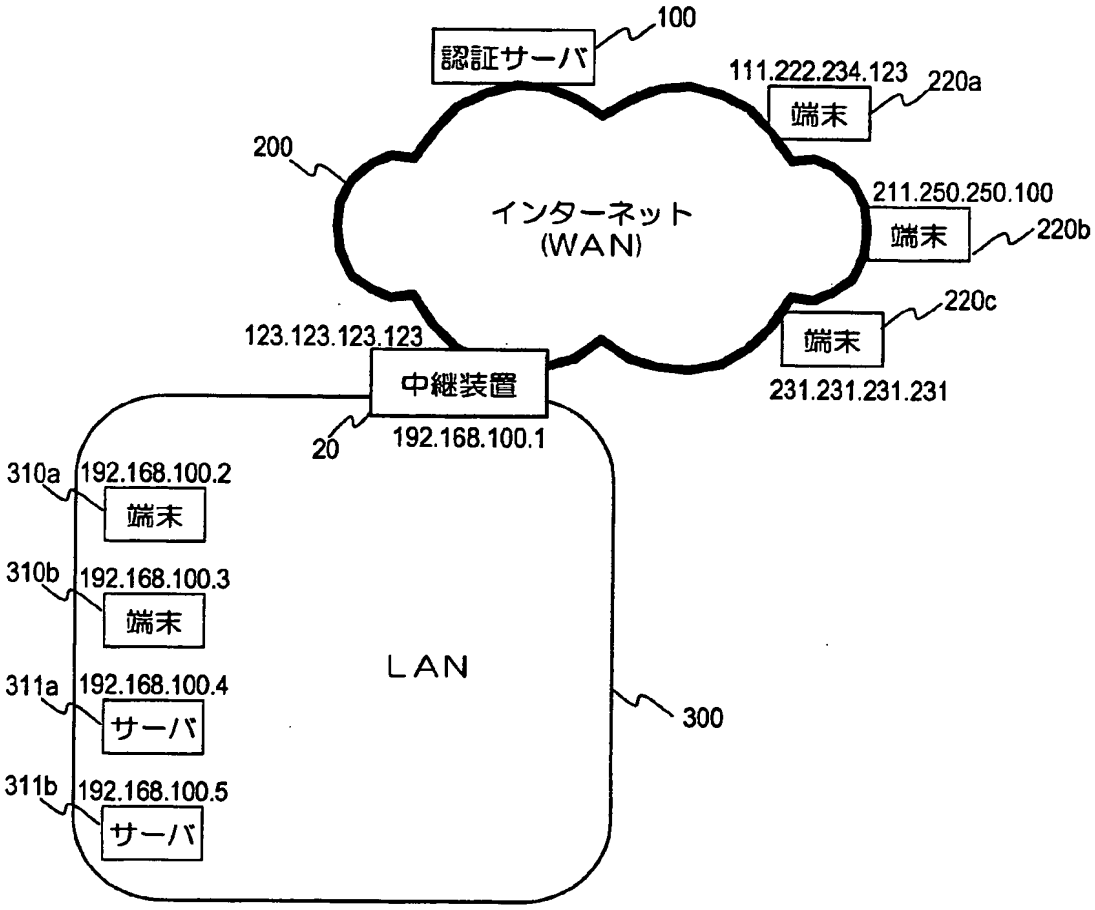

認証サーバ
100
111.222.234.123
端末
220a
200
インターネット
(WAN)
211.250.250.100
端末
220b
端末
220c
231.231.231.231
123.123.123.123
中継装置
20
192.168.100.1
310a
192.168.100.2
端末
310b
192.168.100.3
端末
LAN
311a
192.168.100.4
サーバ
311b
192.168.100.5
サーバ
300

図１７

[図18]

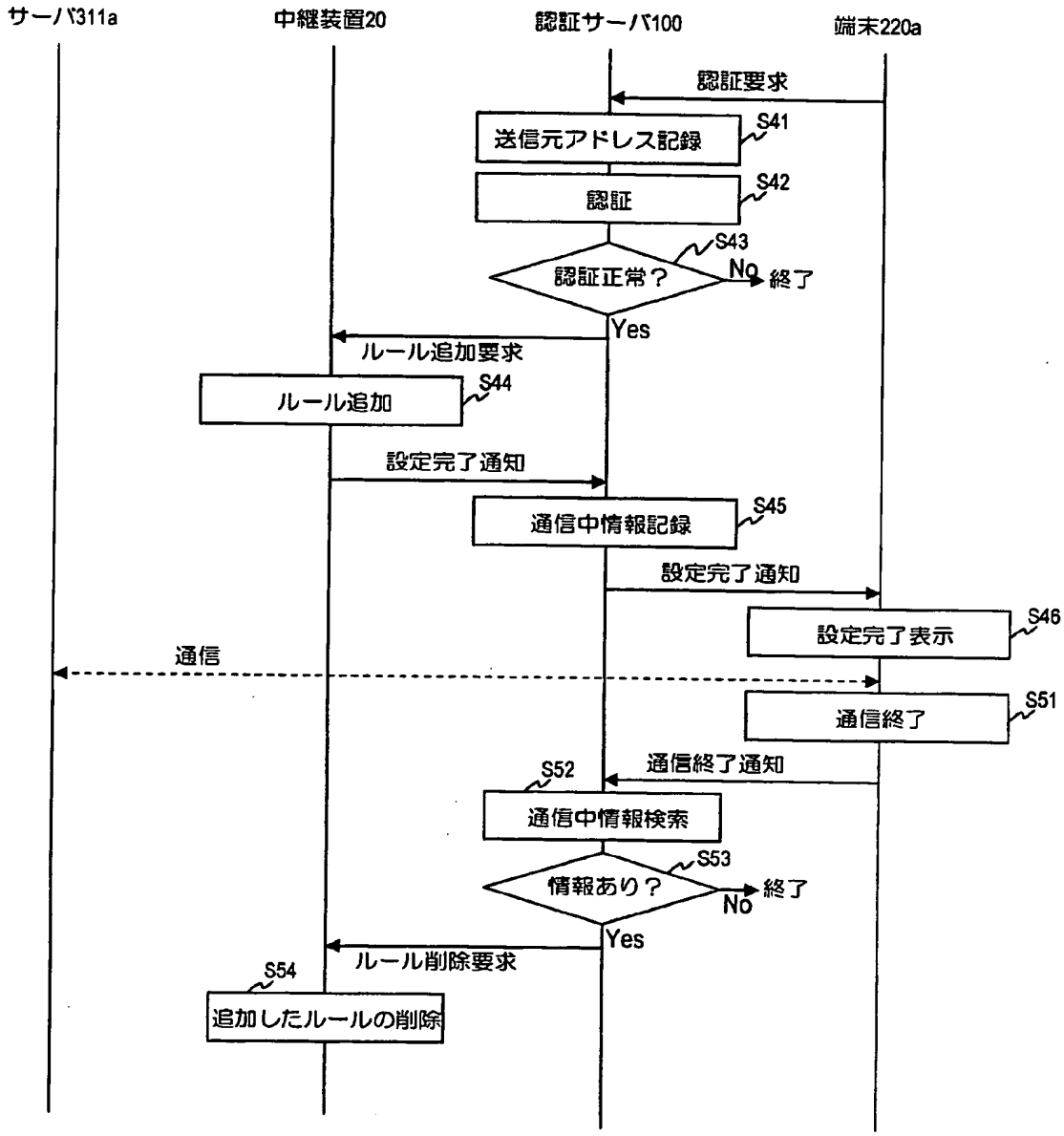

サーバ311a
中継装置20
認証サーバ100
端末220a
認証要求
送信元アドレス記録
S41
認証
S42
S43
認証正常？
No
終了
Yes
ルール追加要求
ルール追加
S44
設定完了通知
通信中情報記録
S45
設定完了通知
設定完了表示
S46
通信
通信終了
S51
通信終了通知
S52
通信中情報検索
S53
情報あり？
終了
No
Yes
ルール削除要求
S54
追加したルールの削除

図１８

[図19]

ソースＩＰアドレス	ソースポート番号	ディスティネーション ＩＰアドレス	プロトコル、 ディスティネーション ポート番号	動作
111.222.234.123	any	123.123.123.123	http	通過

図１９

[図20]

ソースＩＰアドレス	ディスティネーション ＩＰアドレス	プロトコル、 ディスティネーション ポート番号	内部ＩＰアドレス	プロトコルおよび ポート番号
111.222.234.123	123.123.123.123	TCP 80	192.168.100.4	TCP 80

図２０

[図21]

ソースＩＰアドレス	ソースポート番号	ディスティネーション ＩＰアドレス	プロトコル、 ディスティネーション ポート番号	動作
111.222.234.123	any	123.123.123.123	http	通過
any	any	123.123.123.123	https	通過
211.250.250.100	any	123.123.123.123	ssl	通過
any	any	any	any	廃棄

図２１

[図22]

ソースＩＰアドレス	ディスティネーション ＩＰアドレス	プロトコル、 ディスティネーション ポート番号	内部ＩＰアドレス	プロトコルおよび ポート番号
111.222.234.123	123.123.123.123	TCP 80	192.168.100.4	TCP 80
any	123.123.123.123	TCP 443	192.168.100.5	TCP 443
211.250.250.100	123.123.123.123	TCP 22	192.168.100.5	TCP 22

図２２

[図23]

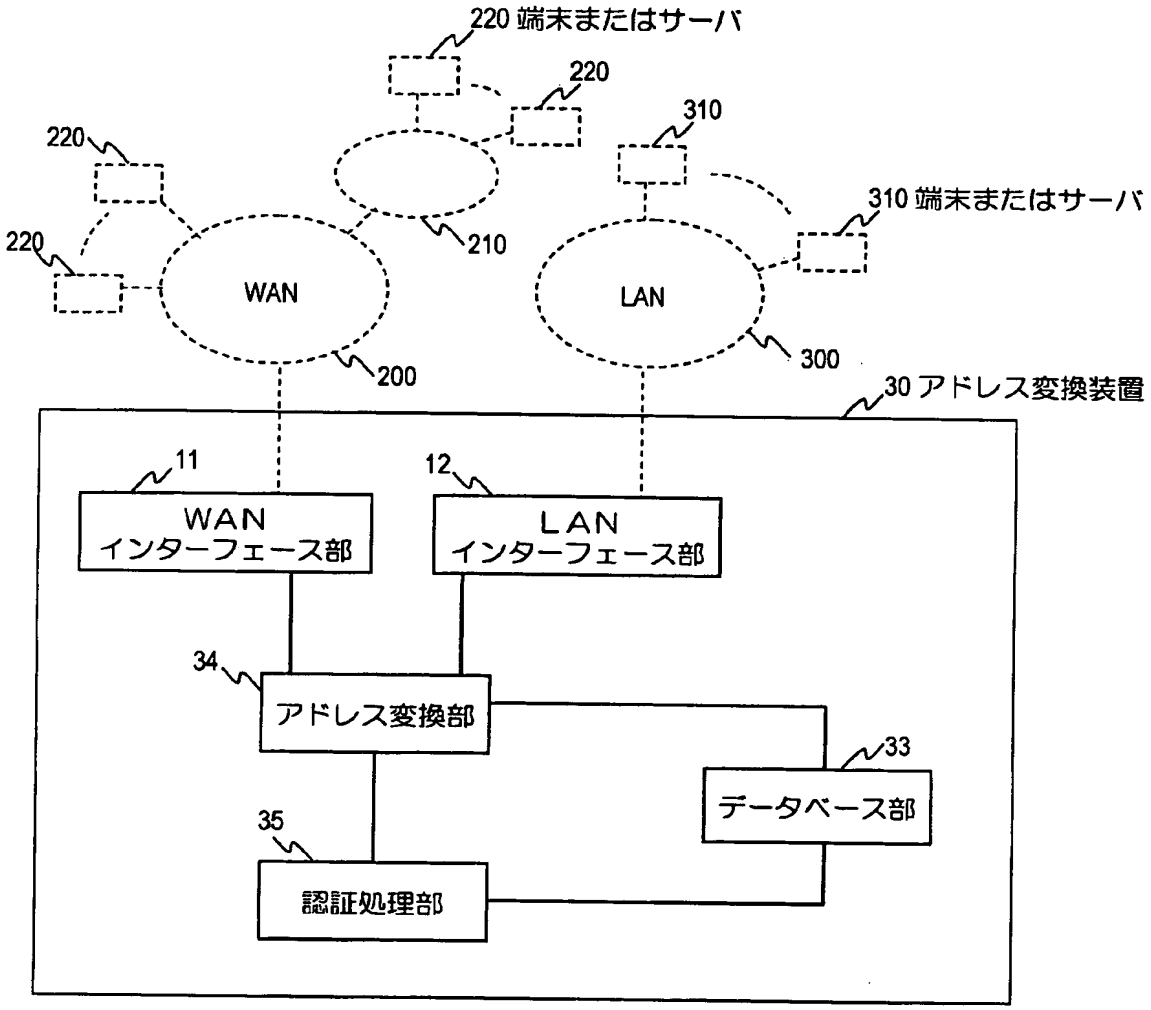

220 端末またはサーバ
220
310
220
310 端末またはサーバ
220
210
WAN
LAN
200
300
30 アドレス変換装置
11
12
WAN
インターフェース部
LAN
インターフェース部
34
アドレス変換部
33
データベース部
35
認証処理部

図２３

[図24]

ソース IPアドレス	ディスティネーション IPアドレス	プロトコル、ディスティネーション ポート番号	内部IPアドレス	プロトコルおよび ポート番号
any	123.123.123.123	TCP 443	192.168.100.5	TCP 443
any	123.123.123.123	TCP 22	192.168.100.5	TCP 22

図24

[図25]

ソース IPアドレス	ディスティネーション IPアドレス	プロトコル、ディスティネーション ポート番号	内部IPアドレス	プロトコルおよび ポート番号
111.222.234.123	123.123.123.123	TCP 22	192.168.100.4	TCP 22
any	123.123.123.123	TCP 443	192.168.100.5	TCP 443
any	123.123.123.123	TCP 22	192.168.100.5	TCP 22

図25

[図26]

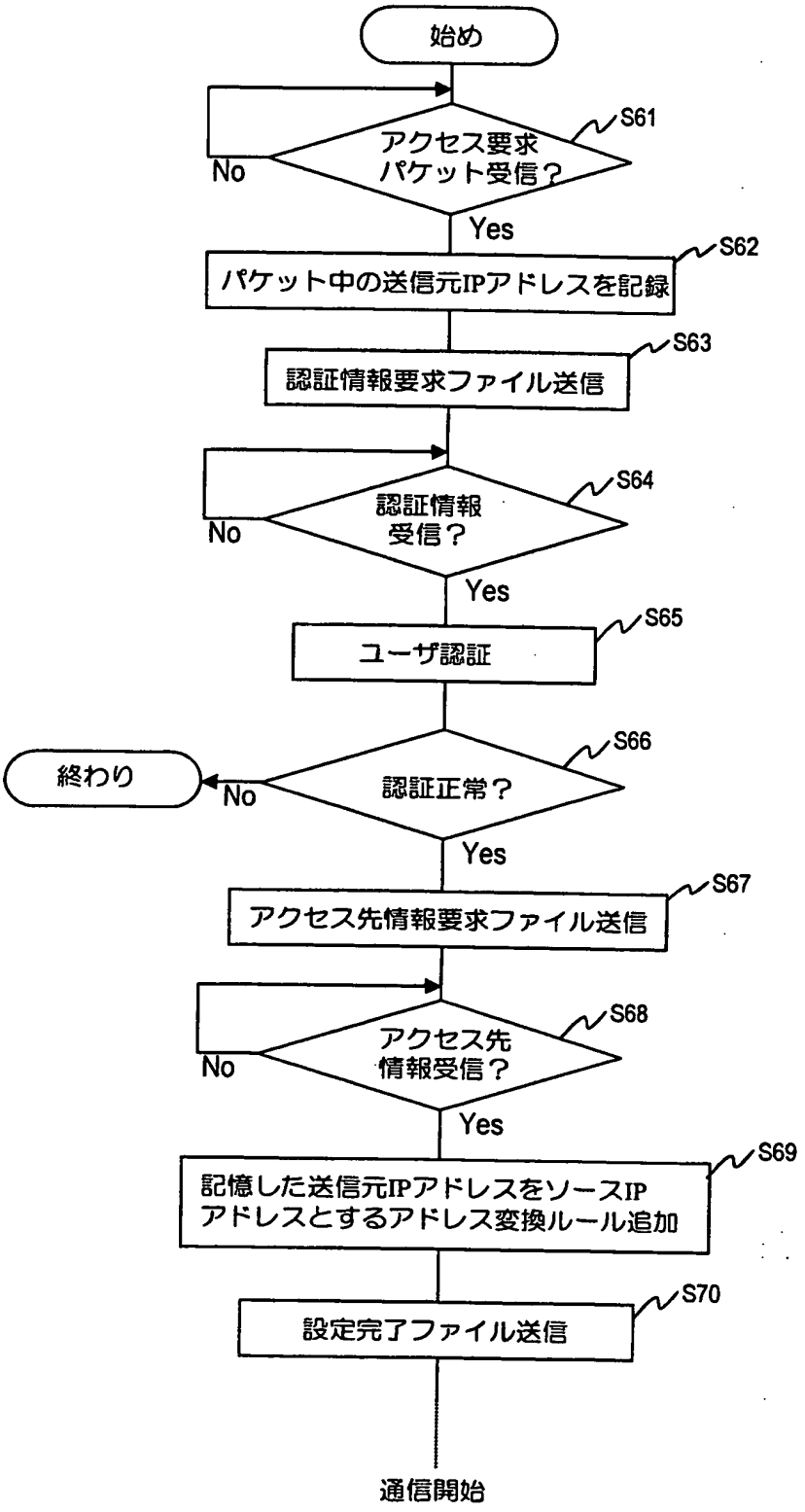

始め
S61
アクセス要求
パケット受信？
No
Yes
S62
パケット中の送信元IPアドレスを記録
S63
認証情報要求ファイル送信
S64
認証情報
受信？
No
Yes
S65
ユーザ認証
S66
終わり
No
認証正常？
Yes
S67
アクセス先情報要求ファイル送信
S68
アクセス先
情報受信？
No
Yes
S69
記憶した送信元IPアドレスをソースIP
アドレスとするアドレス変換ルール追加
S70
設定完了ファイル送信
通信開始

図２６

[図27]

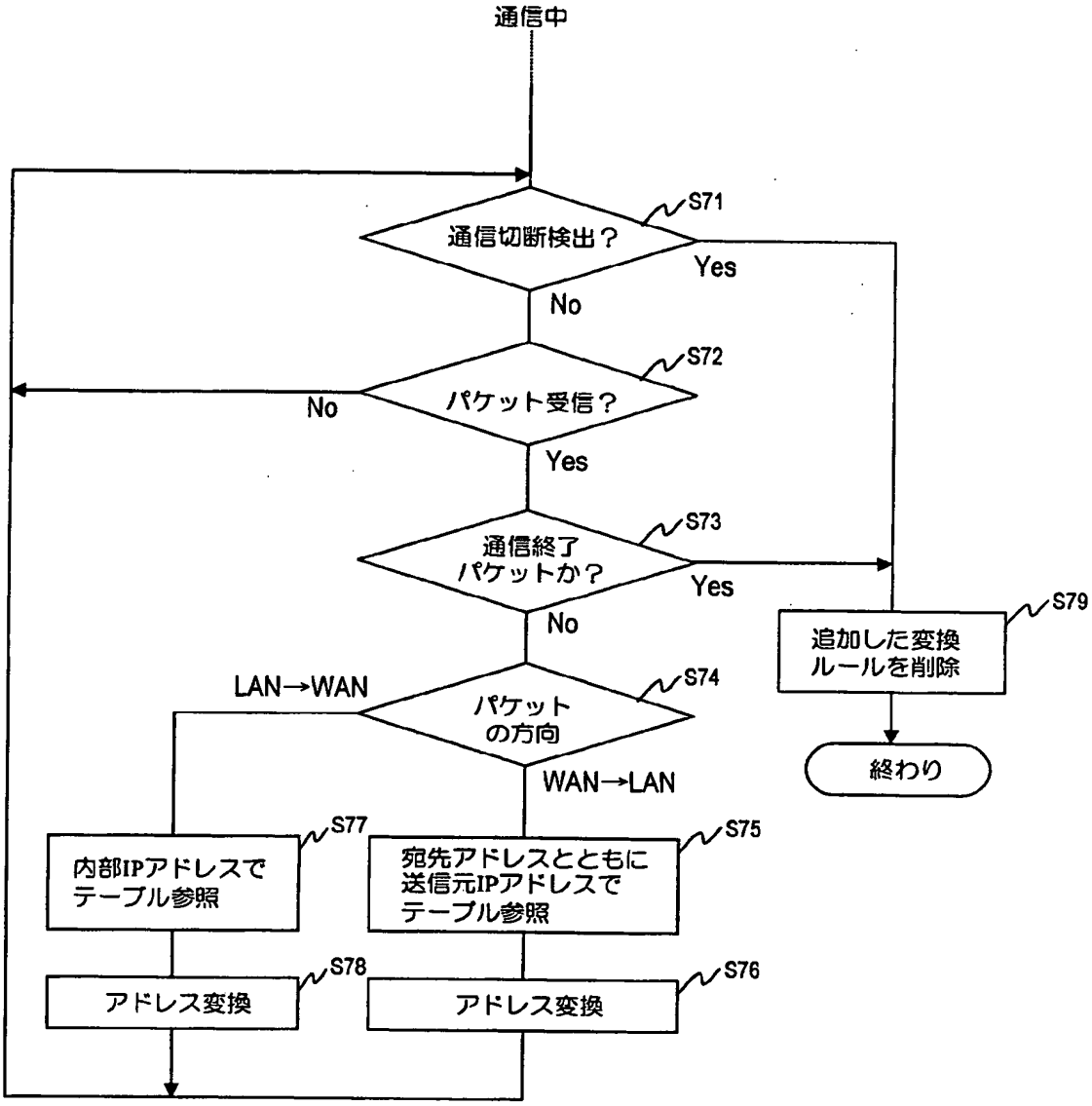

通信中
S71
通信切断検出？
Yes
No
S72
パケット受信？
No
Yes
S73
通信終了
パケットか？
Yes
No
S79
追加した変換
ルールを削除
終わり
LAN→WAN
S74
パケット
の方向
WAN→LAN
S77
内部IPアドレスで
テーブル参照
S75
宛先アドレスとともに
送信元IPアドレスで
テーブル参照
S78
アドレス変換
S76
アドレス変換

図27

[図28]

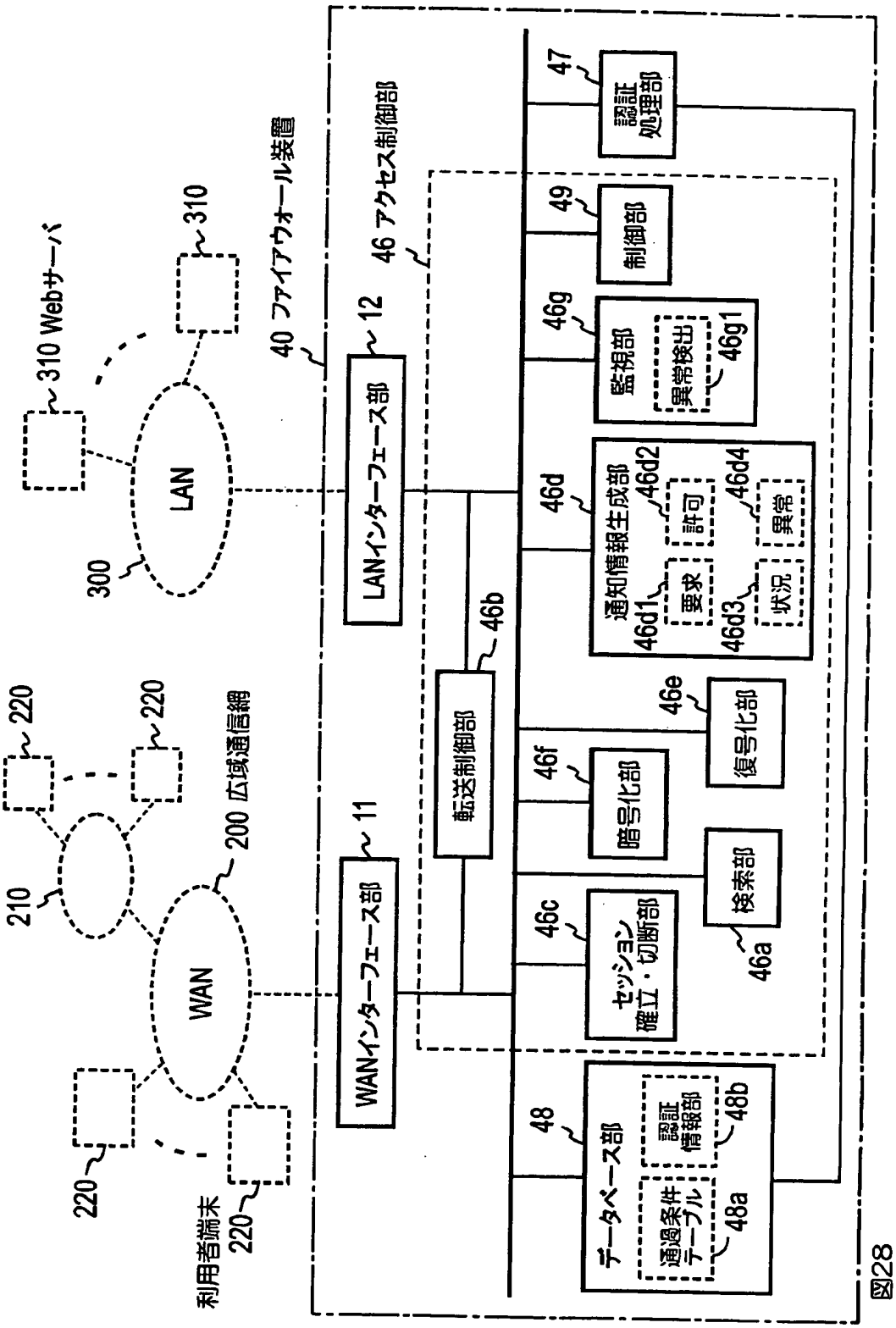

310 Webサーバ
310
LAN
300
40 ファイアウォール装置
12
LANインターフェース部
46 アクセス制御部
47
認証処理部
49
制御部
46g
監視部
異常検出
46g1
46d
通知情報生成部
46d2
許可
46d4
異常
46d1
要求
46d3
状況
46b
転送制御部
46e
復号化部
46f
暗号化部
検索部
46a
46c
セッション確立・切断部
11
WANインターフェース部
48
データベース部
通過条件テーブル
認証情報部
48b
48a
220
210
WAN
200 広域通信網
利用者端末

図28

[図29]

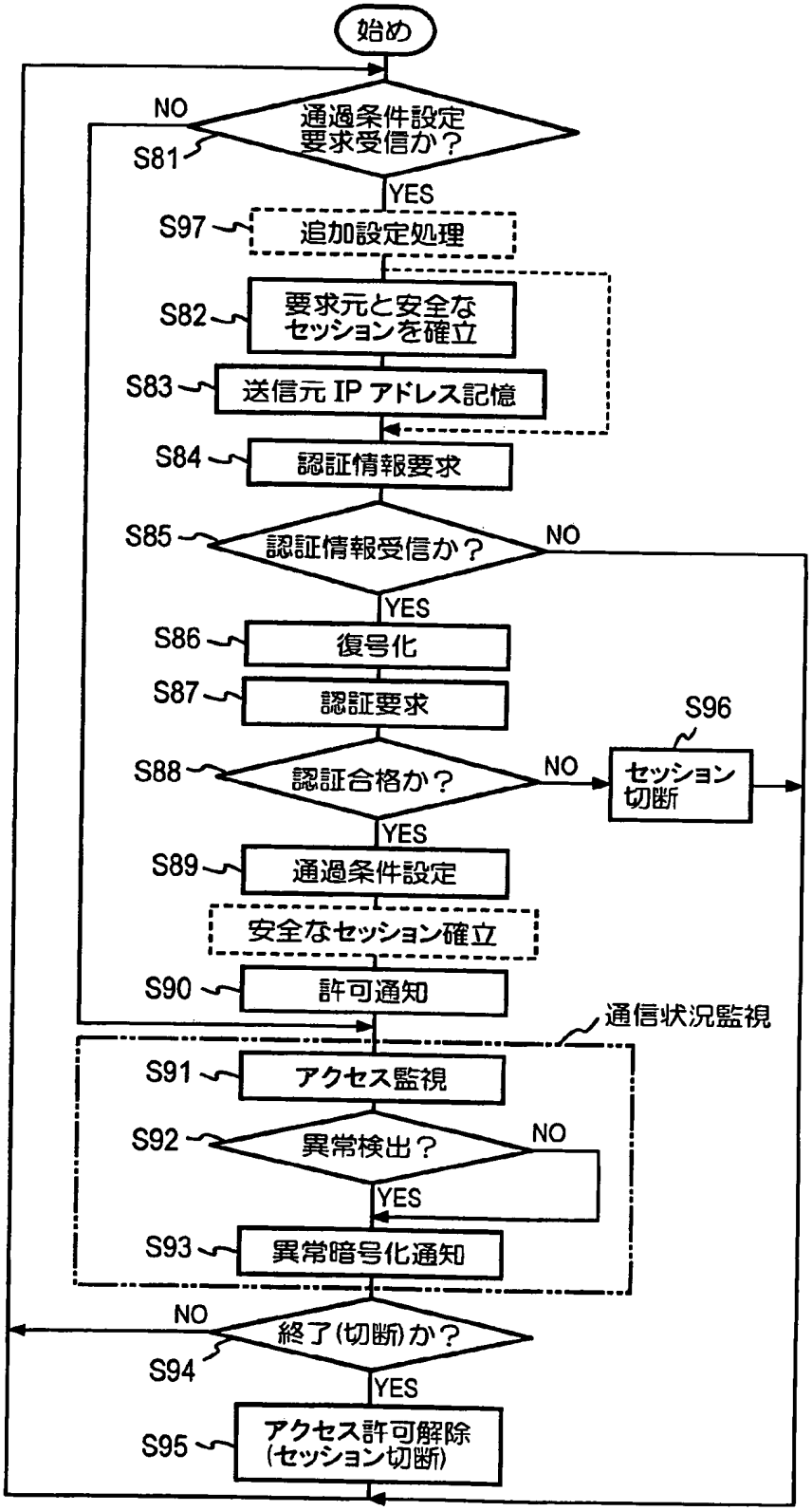

始め
通過条件設定要求受信か？
NO
S81
YES
S97
追加設定処理
S82
要求元と安全なセッションを確立
S83
送信元 IP アドレス記憶
S84
認証情報要求
S85
認証情報受信か？
NO
YES
S86
復号化
S87
認証要求
S96
S88
認証合格か？
NO
セッション切断
YES
S89
通過条件設定
安全なセッション確立
S90
許可通知
通信状況監視
S91
アクセス監視
S92
異常検出？
NO
YES
S93
異常暗号化通知
NO
終了(切断)か？
S94
YES
S95
アクセス許可解除(セッション切断)

図29

[図30]

ソースＩＰアドレス	ソースポート番号	ディスティネーション ＩＰアドレス	プロトコル、 ディスティネーション ポート番号	動作
any	any	111.111.111.2	http	通過
123.123.123.1	any	111.111.111.＊	https(ssl)	通過
any	any	any	any	廃棄

図３０

[図31]

ソースＩＰアドレス	ソースポート番号	ディスティネーション ＩＰアドレス	プロトコル、 ディスティネーション ポート番号	動作
123.123.111.1	any	111.111.111.3	ftp	通過
any	any	111.111.111.2	http	通過
123.123.123.1	any	111.111.111.＊	https(ssl)	通過
any	any	any	any	廃棄

図３１

[図32]

ソースＩＰアドレス	ソースポート番号	ディスティネーション ＩＰアドレス	プロトコル、 ディスティネーション ポート番号	動作
123.123.111.0/24	any	111.111.111.3	ftp	通過
any	any	111.111.111.2	http	通過
123.123.123.1	any	111.111.111.＊	https(ssl)	通過
any	any	any	any	廃棄

図３２

[図33]

ソースＩＰアドレス	プロトコル、ソースポート番号	ディスティネーションＩＰアドレス	プロトコル、ディスティネーションポート番号	動作
123.123.111.0/24	any	111.111.111.3	ftp	通過
any	any	111.111.111.2	http	通過
123.123.123.1	any	111.111.111.2	ssl	通過
any	any	any	any	廃棄

図３３

[図34]

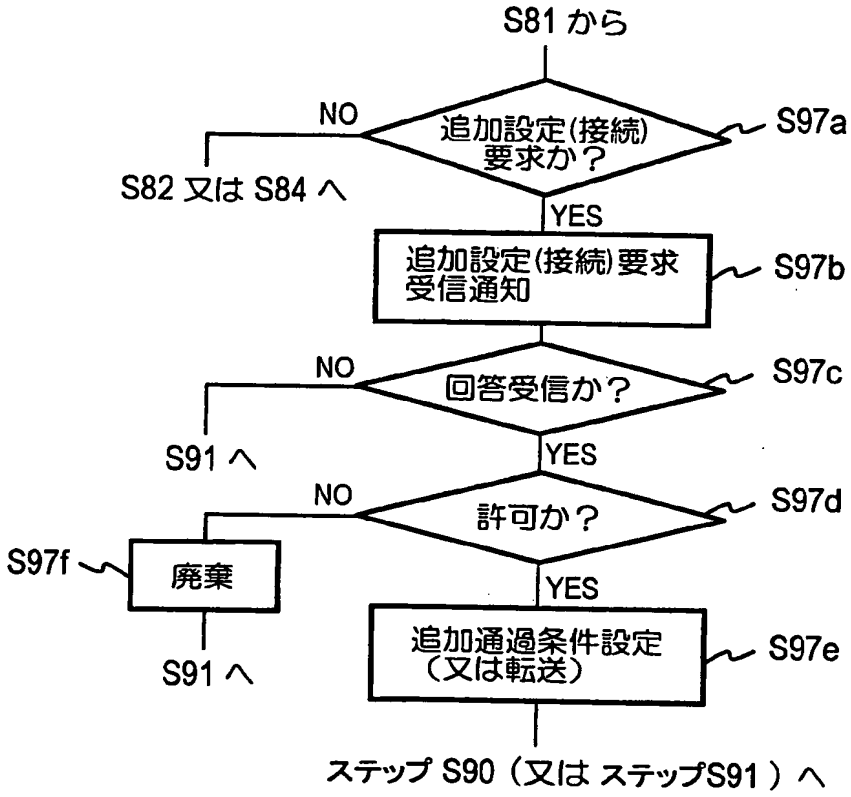


図34

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/007254

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F13/00, 15/00, H04L12/46, 12/66

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F13/00, 15/00, H04L12/46, 12/66

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2003-85059 A (Matsushita Electric Industrial Co., Ltd.), 20 March, 2003 (20.03.03), Par. Nos. [0078] to [0083]; Fig. 6 & WO 2002/076062 A1 Fig. 6 & US 2003/0115327 A1 Fig. 6	1-22
X A	JP 2003-132020 A (Cyber Sign Japan Inc.), 09 May, 2003 (09.05.03), Full text; all drawings (Family: none)	1-12,15-20 13,14,21,22

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 July, 2005 (11.07.05)	02 August, 2005 (02.08.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/007254

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-185517 A (NEC Corp.), 28 June, 2002 (28.06.02), Full text; all drawings & WO 2001/63854 A1	1-10,15-17
A	JP 2002-232450 A (The Furukawa Electric Co., Ltd.), 16 August, 2002 (16.08.02), Abstract; Fig. 1 (Family: none)	1-22

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/007254

Box No. II **Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III **Observations where unity of invention is lacking (Continuation of item 3 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

The matter common to the first group of inventions (claims 1-5) and the second group of inventions (claims 6-10, 15-17) relates to "the address conversion rule" while the third group of inventions (claims 11-14, 18-22) do no have "the address conversion rule".

Next, "the address conversion rule" as the matter common to the first and the second group of inventions is not novel since it is disclosed in the prior art documents (JP 2002-185517 A, JP 2002-232450 A) presented by the applicant.

Accordingly, the first group of inventions (claims 1-5), the second group of inventions (claims 6-10, 15-17), and the third group of inventions (claims 11-14, 18-22) are different inventions.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号 PCT／JP2005／007254

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl.[7] G06F13/00, 15/00, H04L12/46, 12/66

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl.[7] G06F13/00, 15/00, H04L12/46, 12/66

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2005年
日本国実用新案登録公報	1996－2005年
日本国登録実用新案公報	1994－2005年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2003－85059 A（松下電器産業株式会社）2003.03.20，第78－83段落，第6図 & WO 2002／076062 A1，FIG. 6 & US 2003／0115327 A1，FIG. 6	1－22
X A	JP 2003－132020 A（日本サイバーサイン株式会社）2003.05.09，全文，全図（ファミリーなし）	1－12，15－20 13，14，21，22

☑ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 11. 07. 2005	国際調査報告の発送日 02. 8. 2005
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 五十嵐 努 5R 9474 電話番号 03－3581－1101 内線 3565

様式PCT／ISA／210（第2ページ）（2004年1月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ ２００２－１８５５１７ Ａ（日本電気株式会社）２００２．０６．２８，全文，全図 ＆ ＷＯ ２００１／６３８５４ Ａ１	１－１０，１５－１７
Ａ	ＪＰ ２００２－２３２４５０ Ａ（古河電気工業株式会社）２００２．０８．１６，要約，第１図（ファミリーなし）	１－２２

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２００５／００７２５４

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第8条第3項（ＰＣＴ17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

１．☐ 請求の範囲＿＿＿＿＿＿＿＿＿＿ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

２．☐ 請求の範囲＿＿＿＿＿＿＿＿＿＿ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

３．☐ 請求の範囲＿＿＿＿＿＿＿＿＿＿ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第3文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

第１発明群（請求の範囲１－５に係る発明）および第２発明群（請求の範囲６－１０、１５－１７に係る発明）に共通する事項は「アドレス変換ルール」に関するものであるのに対し、第３発明群（請求の範囲１１－１４、１８－２２に係る発明）は「アドレス変換ルール」を備えていない。

次に、第１発明群および第２発明群に共通の事項である「アドレス変換ルール」は、出願人が提示する先行技術文献（特開２００２－１８５５１７号公報、特開２００２－２３２４５０号公報）に記載があるように新規な事項でないことが明らかである。

よって、第１発明群（請求の範囲１－５に係る発明）、第２発明群（請求の範囲６－１０、１５－１７に係る発明）、第３発明群（請求の範囲１１－１４、１８－２２に係る発明）は、それぞれ別の発明である。

１．☑ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

２．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

３．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

４．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☑ 追加調査手数料の納付と共に出願人から異議申立てがなかった。